2001-06

Human factors in Coast Guard Computer Security - an analysis of current awareness and potential techniques to improve security program viability

Whalen, Timothy J.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

HUMAN FACTORS IN COAST GUARD COMPUTER SECURITY - AN ANALYSIS OF CURRENT AWARENESS AND POTENTIAL TECHNIQUES TO IMPROVE SECURITY PROGRAM VIABILITY

by

Timothy J. Whalen

June 2001

Thesis Advisor:	Cynthia Irvine
Associate Advisor:	Douglas E. Brinkley

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Human Factors in Coast Guard Computer Security - An Analysis of Current Awareness and Potential Techniques to Improve Security Program Viability			**5. FUNDING NUMBERS**
6. AUTHOR(S) Timothy J. Whalen			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Coast Guard Telecommunications and Information Systems Command 7323 Telegraph Road, Alexandria, VA 22315			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER** N/A
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The Coast Guard is becoming increasingly reliant upon our nation's information infrastructure. As such, our ability to ensure the security of those systems is also increasing in import. Traditional information security measures tend to be system-oriented and often fail to address the human element that is critical to system success. In order to ensure information system security, both system and human factors requirements must be addressed.

This thesis attempts to identify both the susceptibility of Coast Guard information systems to human factors-based security risks and possible means for increasing user awareness of those risks. This research is meant to aid the Coast Guard in continuing to capitalize on emerging technologies while simultaneously providing a secure information systems environment.

14. SUBJECT TERMS Computer Security, Human Factors, Human Computer Interaction, Coast Guard, Trust, INFOSEC.	**15. NUMBER OF PAGES** 119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HUMAN FACTORS IN COAST GUARD COMPUTER SECURITY AN ANALYSIS OF CURRENT AWARENESS AND POTENTIAL TECHNIQUES TO IMPROVE SECURITY PROGRAM VIABILITY

Timothy J. Whalen
Lieutenant, United States Coast Guard
B.S., United States Merchant Marine Academy, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2001

Author: _____
Timothy J. Whalen

Approved by: _____
Dr. Cynthia Irvine, Thesis Advisor

_____
Douglas E. Brinkley, Associate Advisor

_____
Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Coast Guard is becoming increasingly reliant upon our nation's information infrastructure. As such, our ability to ensure the security of those systems is also increasing in import. Traditional information security measures tend to be system-oriented and often fail to address the human element that is critical to system success. In order to ensure information system security, both system and human factors requirements must be addressed.

This thesis attempts to identify both the susceptibility of Coast Guard information systems to human factors-based security risks and possible means for increasing user awareness of those risks. This research is meant to aid the Coast Guard in continuing to capitalize on emerging technologies while simultaneously providing a secure information systems environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The Coast Guard and our nation as a whole are becoming increasingly reliant upon our information infrastructure. As we do so, our capability to ensure the security of the involved systems increases dramatically in import.

Traditional security measures focus on system-oriented concepts that, in theory, may provide safe, secure systems in and of themselves. However, systems do not operate in a sterile environment and human interaction is a critical component of any viable system.

Malicious code, intrusion techniques, and other attacks often rely upon the human side of the Human Computer Interaction (HCI) chain. If mitigating security measures are focused solely on remedies oriented toward the system side, the problem that actually led to the compromise may continue to propagate. This tendency is clearly displayed in the spread characteristics of most modern viruses, such as the recent "I LOVE YOU" virus, since they rely upon a user to open and, thereby execute, a suspect file. It is also demonstrated in password cracking techniques that exploit consistent procedural errors made by users. Updating virus definitions, establishing policy addressing password selection and similar measures are designed as security patches. Patching an exploited security hole, however, does not change the characteristic behavior that made the system susceptible. In fact, concentrating solely upon system-side solutions could in fact encourage lackluster compliance with recognized safe computing practices and actually result in lower level of overall security.

Security patch solutions also cause additional problems. In order for patch-based solutions to be effective, they must be installed and used correctly. This is not always the case. This leads to another human factors issue that is not limited in scope to end users. Network system managers often fail to install, or inadvertently overwrite the most current security patches during reinstallation of software. Users of all sorts fail to keep current virus definitions up to date. Clearly demonstrating the problem within the government/military communities, in a May 2000 meeting, members of U.S. Navy's Fleet Information Warfare Center (FIWC) stated that the majority of identified successful network attacks would have been prevented had the targeted systems and users used the most current security patches, virus definitions, and policy instructions. In fact, the Navy has released information indicating that "nearly half of computer intrusions...could have been prevented had users followed two simple rules: 1. Do not click on attachments, and 2. Use strong passwords" [Ref. 1]. The fact that systems do not have effective security mechanisms and are a patchwork of security retrofits that must be maintained by users and poorly trained administrators makes human factors crucial.

Another consideration is the affect of information security policy upon the organization's business practices. Information systems exist for the primary purpose of supporting an organization's business practices. Similarly, information system policy should support the use information systems that enhance achievement of business goals. They should not prevent achievement of those goals, place excessive burdens upon users leading to frustration, or cause the policies themselves to be circumvented.

This consideration becomes increasingly important as the role of information systems expands in today's environment. As an organization's information systems

capabilities grow and expand, security policies relating to those capabilities must change as well, lest restriction of goals occur. One example is shown when examining previously restrictive policies regarding remote access of computer systems. While seemingly acceptable in the early stages of the organization's development, Federal law now mandates implementation of telecommuting policies for federal workers thus making this a new-found objective for all government bodies. Policy changes that allow support of this new goal may be necessary.

The questions follow: To what extent do user habits, impressions, and practices contribute to an organization's ability to provide a safe, secure information infrastructure; and to what extent do they prevent the organization from capitalizing upon information systems in accomplishing their business goals? To analyze that risk with respect to the Coast Guard, these factors need to be identified and measured. Once made, that measurement can be used to gauge the potential for compromise and better assess the focus of its efforts to provide security while simultaneously sponsoring (as opposed to stifling) growth through expanded use of new and emerging technologies.

Risk analysis based upon collected data could allow an organization to identify critical human factors-based weaknesses, identify sub-populations within an organization who might be more susceptible, and better assess the results of current security practices and policies. A better understanding of the human nature of the system users should allow the organization to better manage the HCI-based security risks.

B. PURPOSE

Congress has seen the need to establish specific legislation on the subject of Information Security. In fact, the *Government Information Security Act of 1999* clearly

identifies the need to model the government's comprehensive information infrastructure upon "the 'best practices' of leading organizations in the area of information security." [Ref. 2] Measures required by the act are established with clear knowledge of the current and increasing role of networked information systems within our government and economy. In passing the legislation, they clearly noted that the General Accounting Office currently lists "government-wide information security on its list of 'high risk' government programs," and as a branch of the Department of Transportation, the U.S. Coast Guard is fully subject to the criteria outlined within the act. Additional responsibilities and guidelines are provided for other branches including the Department of Defense, the Central Intelligence Agency, and the Department of Justice.

The *Government Information Security Act of 1999* provides requirements for an annual independent assessment of the security climate within the government and provides that the General Accounting Office (GAO) can accomplish this assessment. In September 2000 the GAO released audit results for the year 2000. They found a number of severe weaknesses as summarized below in Figure 1.

As shown, the range of security weaknesses found in each branch of the government was significant. In December 2000, the GAO went further when it released a specific report focusing on the Coast Guard's entire IT environment. The report, *Information Technology Management, Coast Guard Practices Can Be Improved* includes recommendations for improvements in each of five key areas among which is information security. Specifically, the report identifies shortcomings within the areas of risk assessment, information security awareness, controls, evaluation, and central management. [Ref. 4]

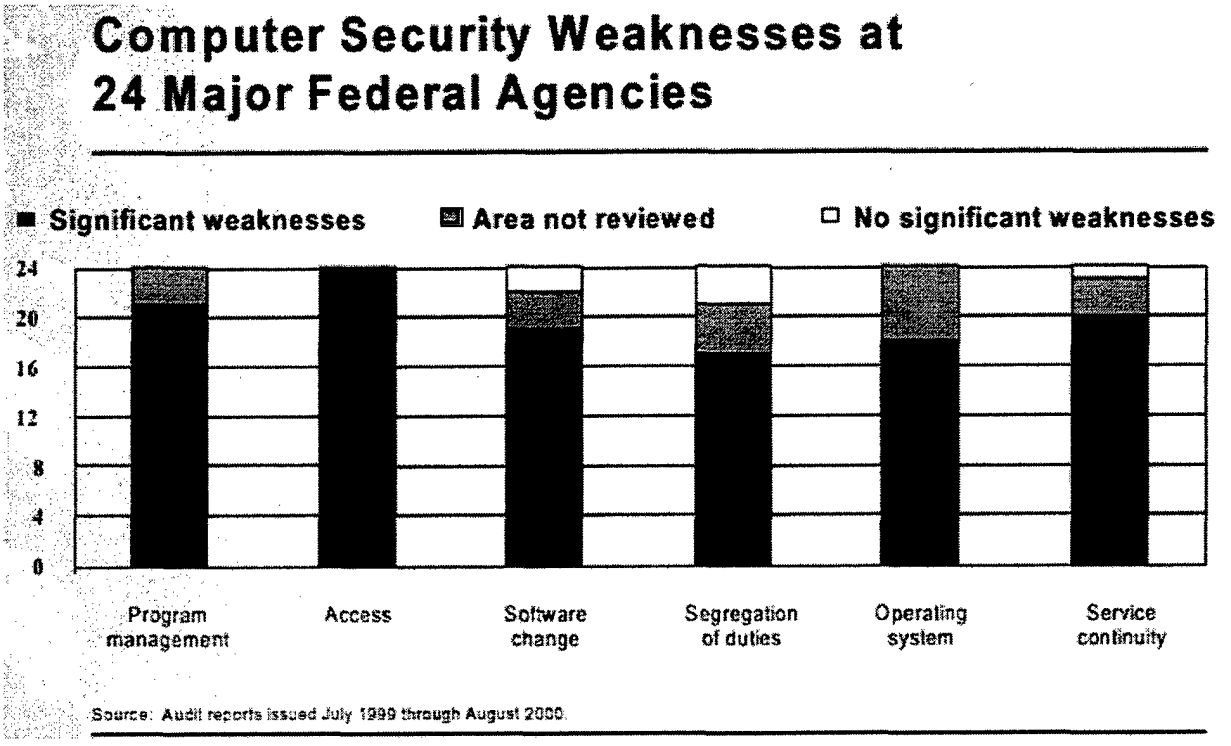


Figure 1. Federal Agency Computer Security Weaknesses from: [Ref. 3]

The Coast Guard is rather unique within the government in that its mission structure is extremely diverse. Among its missions, several clearly have a heightened need for protection including its military, transportation, and law enforcement roles. In addition, the Coast Guard maintains significant stores of records containing Privacy Act protected information all of which must be protected from compromise.

Sharing these roles expands the variety of e-Government programs which are currently in place and which are being developed. The computer user community present in the Coast Guard therefore becomes quite diverse as members from all communities interact with these systems. While the primary system used, a Windows NT based system bundled with Microsoft's Office '97 suite, there are a variety of other applications that are normally used and user training and knowledge levels vary greatly.

Identifying the perceptions and practices of a diverse range of users will serve to assist the Coast Guard in focusing its efforts to address the concerns expressed by the GAO. Specifically, this study is intended to serve as: a preliminary human factors-based risk assessment; a gauge of users' current perceptions with regard to information security awareness; and a measure of actual user practices. The objective of the study is to provide information that will be valuable to management in evaluating potential solutions to the concerns that were raised by the GAO.

C. ORGANIZATION OF STUDY

1. Methods of Assessment

In order to satisfactorily perform this study, the current information security awareness environment needs to be assessed. There are a variety of methods for assessment with advantages and disadvantages for each.

Non-obtrusive measurement, through passive observation of the user population performing within their normal work environment, can serve as a valuable research tool. Participants do not change their behavior since they are unaware that they are being observed. Although it has the potential to demonstrate the actual performance of participants, a study conducted in this manner is extremely time consuming and costly and there is no guarantee that all of the desired potential weaknesses will be observed within a given time frame. For this reason, this method is infeasible for the purposes of this study. However, having worked within the environment himself, the author has had an opportunity to make some observations with regard to normal working habits of Coast Guard information system users.

Surveys provide another means of assessment. In general, surveys can be used to identify general areas of concern. However, assuming that the "right" questions are asked, surveys can provide can provide more focused results. In this respect, the strength of a survey is largely dependent upon the strength of its development. Drawing upon other research can help to refine a survey to focus on previously identified potential problem areas. In addition, since, as mentioned before, the author has worked within the information systems environment being assessed, direct experience can aid in probing perceived potential problem areas.

A disadvantage posed by surveys of computer security environments is the increased potential for a "fear factor" which might cause users to answer with what they feel is the correct answer according to policy vs. what they actually perceive as the truth. This often stems from mistrust on the part of those surveyed that their answers will be used against them. Within hierarchical military environment, this can prove to be even more critical. Failure to address this tendency in survey respondents could skew results and have adverse affects upon a survey's potential to clearly and properly identify areas of concern.

A third method of assessment is to assign users a specific set of tasks within a controlled environment and observe their attempts to work through those tasks. One of the studies referenced in the course of this study, *Usability: A Case Study* [Ref. 5] makes extensive use of this method. Since the area of focus of that study was relatively narrow in that its goal was evaluation of PGP 5.0 software in depth, this method worked very well studying that particular instance. Here our scope is much broader in that it will

attempt an assessment of a wide range of users performing diverse tasks. For this reason, extensive use of task assignment method would not be feasible.

By capitalizing on experience and other bodies of research such as *Users Are Not the Enemy,* [Ref. 6] focusing on password use deficiencies, *Creating Trust*, [Ref. 7] which addresses user trust on the web, and the previously mentioned, *Usability: A Case Study*, the author feels that a viable survey can be constructed to assess the skills, perceptions, and practices of Coast Guard information system users. Through assurances to personnel regarding anonymity and the purpose of the study, as well as the fact that this study is being conducted independent from the Coast Guard command structure, the author feels that the "fear effect" can be minimized. Supplementing the survey with practical skills exercises and follow-on questioning of participating users will assist in verifying and refining survey results.

2. Population Selection

Due to the diverse nature of the Coast Guard's missions, any sample population would have to be representative of this situation since education and skill levels have the potential to vary greatly within these communities. Based upon the sponsorship of the Coast Guard's Telecommunications and Information Systems Command (TISCOM) and the office of the Chief Information Officer, willing participation by four diverse units was obtained. These units are as follows:

1. The Coast Guard Human Resource Service and Information Center (HRSIC) focused primarily toward administrative and technology support functions;

2. The Coast Guard Marine Safety Office San Francisco Bay, which is focused on the Coast Guard's Marine Safety functions including vessel inspection, accident investigation, marine environmental protection, mariner licensing, and critical incident planning;

3. The Coast Guard Air Station San Francisco providing search and rescue and air support for Coast Guard operations; and

4. The Coast Guard Station Monterey Bay, engaged in duties which include the search and rescue and law enforcement mission areas as well as providing support to the environmental protection mission and assisting other local and federal agencies.

D. OUTLINE OF THESIS

This thesis is comprised of this and three additional chapters as follows.

Chapter II – Data Collection and Measurement Methodology: This chapter will focus on the methodology used in the course of this study. Specific attention will be given to identification of human factors concern areas, survey composition, and other means of assessment used in the course of the study.

Chapter III – Presentation and Analysis of Collected Data: This chapter provides a statistical breakdown of survey results. Comparisons are made between differing groups within the sample and assessments are made against established safe computing practices.

Chapter IV – Conclusion and Recommendations: Based upon conclusions drawn from data collected in the course of this study, this chapter attempts to provide

recommendations for future security policy decisions which may enhance security while simultaneously allowing the Coast Guard to capitalize on expanded use of technology.

Appendix – Human Factors Survey: Contains a copy of the survey completed by the participants of this study.

II. DATA COLLECTION AND MEASUREMENT METHODOLOGY

A. INTRODUCTION

Gauging user awareness of a subject can prove to be a difficult assessment. Any assessment must be narrow enough to be of use while at the same time broad enough to accurately identify user perceptions that might affect the subject matter. The remainder of the this chapter will discuss the methods used in an attempt to strike a balance which captures user perceptions regarding specific security concerns. Upon identification of these areas of concern, specific methods of assessment are discussed with regard to their implementation in this study.

B. IDENTIFICATION OF POTENTIAL AREAS OF CONCERN

When analyzing security from a human factors perspective, it is necessary to focus not only on the problem, but on reasons behind the problem. It is often necessary to ask why users are performing one action when they should be performing another. If the system, training program, policy, or some other factor creates a tendency in users which is contrary to the system goal, a human-factors based solution would not address the user's tendency, but would focus on the item creating that tendency.

In the case of information security, the process needs to examine all points of human interaction within which a failure could lead to vulnerability. Among the areas which should be examined are the actual practices of users which create vulnerabilities, user security perceptions of both the systems they are using and the policies that apply to those systems, user knowledge, training, and awareness levels and, the user interface.

1. Security Practices

Information security practices can be examined from a number of perspectives. In fact, the System Administration, Networking and Security Institute (SANS) distinguishes between end users, senior executives, and information technology workers when identifying *Mistakes People Make That Lead to Security Breaches* [Ref. 8].

The vast majority of Coast Guard system users fall within the "end user" category. In fact, for many purposes, senior executives and information technology workers still operate as end users as well. In this respect, their habits are no less important than those of other end users. For this reason, this study will focus on the perceptions and practices of end users. In their list of mistakes, SANS identifies the top five security mistakes in this category as: 1. Opening e-mail attachments without verifying their source and checking their content; 2. Failure to install security patches; 3. Installing games, and screensavers from unknown sources; 4. Not making and testing backups; and 5. Using a modem while connected through a LAN. [Ref. 8]

Noticeably absent from the SANS listing is the mention of passwords. CISCO systems criticized SANS for removing password flaws from the list and, in response published its own listing of the *Top 10 Cyber Security Tips for Security Managers and IT Departments* [Ref. 9]. In this list, Cisco places special emphasis on strong passwords and password change policies by placing them as the first two items on their list, justifying this with the fact that a significant percentage of remote break-ins are the result of bad passwords. Like SANS, CISCO also ranks installation of security updates and the tendency of users to open attachments as posing a high security risk. [Ref. 9]

The Coast Guard's implementation of the Windows NT environment locks out the host computer's "C:" drive and requires network storage. This places backup functions in the hands of system administrators. In addition, modems are not included in the Coast Guard's deployment of its NT workstations. By eliminating these two items, the end user concerns expressed by CISCO and SANS encompass:

1. Password implementation and use;
2. Opening suspect e-mail attachments;
3. Failure to Install Security Patches; and
4. Installing software from unknown sources.

The potential for security breaches caused by weaknesses within each of these categories varies based upon various factors. A further discussion of each category and potential for human factors weaknesses follows.

a. Passwords

Passwords currently serve as the primary means for system user authentication within the Coast Guard's computing environment. However, use of a password does not, guarantee the identity of the user, and as stated above, industry experience has shown that the use of "bad passwords" has led to significant security lapses in the past. In *Users Are Not the Enemy,* Anne Adams and Martina Angela Sasse identify several categories that lead to weaknesses in password-based authentication systems. Both the number of passwords the individual uses and the construction or content of the password itself were identified as major concern areas as were users

perceptions with regard to passwords, their purpose and use within the organization. [Ref. 6]

A user's ability to remember multiple passwords decreases as the number of passwords they are required to know increases. Adams and Sasse found that the maximum number of passwords that could be effectively managed for most users was about 5, and this was dependent upon the password's use frequency as infrequent use of passwords reduced the users ability to remember them.

The Coast Guard's Information Systems Architecture relies on passwords beyond the initial Windows NT logon. The Marine Safety Information System (MSIS), Law Enforcement Information System (LEIS), and other similar networked database systems have additional, password-based authentication schemes. Personnel accessing Department of Defense resources remotely have passwords for those systems as well. In general, the number of password-based systems a user interacts with at work is largely dependent upon the individual's occupation.

In today's environment, password use is not limited to systems at work. Users also may have passwords for systems at home. As use of the Internet grows and practices such as online shopping, banking, web-based e-mail, site registration, and other forms of secure interaction take hold, the number of passwords used outside the work environment grows as well. Since this has the possibility of greatly increasing the number of passwords a user must memorize, it becomes important to consider the number of passwords that a user has outside of work as well.

The ability of a user to construct a strong password is equally important. Weak passwords are easily broken and therefore provide little value as a means of

authentication. The use of English and foreign dictionary words, keyboard strings, names, acronyms, and personal information such as a birth date or social security number all serve to create weaker passwords.

From the user perspective, passwords have to be memorable to be of use. Unfortunately the techniques users create to make their password memorable are often the same techniques historically used by password crackers. However, since cryptic passwords are more difficult to remember, users often continue to create weaker, easy-to-remember passwords.

Some systems, such as MSIS attempt to solve this problem by randomly generating passwords. However, systems such as this can cause more problems since users often have difficulty remembering these system-generated, "strong" passwords and, as a result, are forced to write them down to avoid system lock out.

In an ideal password-system world, users would have separate, strong, memorable passwords for each system they are using. However, users themselves recognize their own memory weaknesses and attempt to compensate through a variety of techniques. Users may link the passwords they use on diverse systems through a common theme (i.e. USCG4vr.1 for system 1, USCG4vr.2 for system 2, etc...). In the worst case, users may use the same password on multiple systems. In this case, a single password compromise would leave each of the remaining systems vulnerable.

To minimize the risk of possible compromise, password policies are usually written which require the periodic changing of passwords. Within the Coast Guard's Windows NT environment, the network system manager accomplishes this by setting a password expiration date. At the time the old password expires, the user is

prompted to enter a new password. However, most policies also direct users to change their passwords should they feel that it has been potentially compromised. Since the system cannot predict the occurrence of this situation and thereby provide a prompt screen as it does at password expiration, users should be aware of the proper procedure for performing this action. Unfortunately, this information is not normally provided to users when they initially receive system access, and for most users, it is not a common practice. As such, there is a strong potential that many users would not know how to change their own passwords should they be compromised. If this is indeed the case, it would form the basis of a significant flaw in the password-based authentication scheme currently in place.

b. Opening of Suspect E-Mail Attachments

The spread of malicious code through the use of e-mail has become pervasive. In fact, the opening of infected e-mail attachments is the most prevalent means of virus infection today. Since new viruses taking advantage of this are regularly finding their way into the wild, merely scanning for infected attachments cannot completely address the problem.

In order to properly attack this problem while simultaneously maintaining productivity, users must be able to reasonably assess the contents of an e-mail attachment prior to opening it. In order to do this, the user must be aware of several issues with regard to virus infections.

First, the user must be able to determine the file type of the attachment. In the Windows environment, this is done in two ways. The Graphical User Interface (GUI) provides a visual key as to the application associated with the file type. For instance, a

Microsoft Word document attachment will have a small icon displaying the blue "W" associated with that program. For file types that a user is familiar with, this can quickly help them determine the expected application it will open with. The problem with this is that it is not always readily apparent to the user what application is opening the file. In fact, the file may, by its very nature, be self-executing.

Windows NT uses the file extension to determine how the operating system will execute a particular file. For example, Windows NT will use Microsoft Word to open a file named Report.DOC since the .DOC extension is associated with Microsoft Word. By default, Windows hides this file extension for "known" file types, that is file types with an application associated with them in the Windows NT registry. For a user to ensure that the file type of the attachment is known, they must make the conscious effort to prevent the system "hiding" these file type extensions. Several viruses actually make use of this default setting in an attempt to lure users into believing they are of benign content. Viruses such as the recent HOMEPAGE.HTML.VBS may appear in a user's e-mail inbox without their extension. In this case, the attachment would appear to be titled HOMEPAGE.HTML. An unsuspecting user might open the file with the assumption that the file is merely a web page and not the visual basic script file which is easily revealed by examining the "real" file extension.

Having determined the contents of file, the current architecture requires the user to know whether or not the particular file is capable of containing malicious code. In his article *Infectable Objects,* Robert Vibert provides a history of viruses and discussion of historical spread methods, there are "over 180 distinct file types and other objects which viruses could target or hide within." [Ref. 10] While many of the file types

are rather obscure, many are among the more common files in use by ordinary users today. For instance, .DOC, .XLS, and .PPT represent the file extensions for Microsoft's Word, Excel, and PowerPoint respectively. Each of these file types can potentially carry Macro viruses. Prior to making the decision as to whether or not to open a file attachment, the user should, at the very least, be able to recognize that the file is *capable* of containing malicious code.

Finally, assuming that a user has been able to determine both the file type and its capability to carry malicious code, there is still another decision to be made. Should the file be opened at all? To determine this, the user must assess the e-mail itself, which leads to a number of other questions: Were the correspondence and the attachment expected? Is the sender known, and if not, is it normal to receive e-mail from unfamiliar sources? Does the subject line appear legitimate? Can the origin of the e-mail itself be determined? The answers to each of these questions can provide critical information. Historically it has been shown that: viruses such as the ILUVYOU can spread to all known users in an Outlook address book so that the message comes from a familiar person, however, the correspondence and attachment are not of an expected type; unfamiliar users may target a user or users with malicious attachments; viruses spreading through e-mail often contain subject lines which attempt to entice the user into opening the attachment with no real explanation of the content; and e-mail spoofing techniques easily allow persons with malicious intent to forge e-mail messages so that they appear to have been genuine.

A user who can collect and assess that information can better determine whether or not to suspect a particular attachment. If all users were able to properly assess

incoming attachments before deciding to open them, e-mail attachment based infections could be expected to drop dramatically. If users proceed without the knowledge and awareness necessary to make these decisions while the environment remains the same, the likelihood is that this will remain a highly vulnerable area.

c. Failure to Install Security Patches

In today's computing environment, applications and operating systems are regularly released with bugs and security holes. In many cases, service packs and patches soon follow the software release. The problem is that these bugs and security holes are left in place unless the user actually acquires and installs the available patches.

From the point of operating system and application software in the work environment, this is primarily the responsibility of the Coast Guard's IT staff. However, if telecommuting and remote access become more common, more of this responsibility is shifted to the end users since Coast Guard IT personnel would not have access to those remote systems.

Even without considering remote connections, the Coast Guard must concern itself with the practices of end users at home if those users exchange material between their work and home systems. Users transferring data via floppy disk or e-mail increase the vulnerability of Coast Guard systems when the users fail to maintain up-to-date virus definitions or, for that matter, fail to have anti-virus software installed at all.

Today, many software companies provide various "automatic" means of ensuring they are current. The Windows Update feature which ships with Windows 98/Me and the LiveUpdate scheduling feature included in Norton's Antivirus

are examples of this type system. This would seem to remove the burden from the user since the software handles these functions, but this is not completely the case.

If the user has decided to activate the critical update notification function, Windows Update will notify a user of a "critical update" when that user is connected to the Internet. However, it does not force users to download and install such updates. Many of these updates, especially those for the operating system and web browser, can be extremely large to download, especially over a slow modem connection.

Norton's LiveUpdate also relies on the user to assist it in performing its "automatic" function. When setting up a schedule, Norton prompts the user to choose a frequency for using the LiveUpdate feature. This feature communicates with the Symantec web site to determine if the Antivirus software itself and the virus definitions are current. If they need to be updated, the software will download the updates and install them. In order to be effective, the user must establish a frequency that ensures that the virus software and definitions are current. However, other steps need to be taken as well. If the user schedules the LiveUpdate function to check for virus definitions during night hours, the user must ensure that the system is left on so that the action can take place. In addition, if the user connects to the Internet via a dial-up Internet Service Provider (ISP), the ISP password must be stored on the user's system. If it is not stored, the LiveUpdate process will halt at the user sign-on screen since the lack of a password will prevent Internet access from occurring. Finally, in order to ensure that the virus definitions are current, and to provide protection for rapidly-spreading, new viruses, the user should periodically manually attempt to verify the status of the updates.

A failure in any of the above areas can not only weaken the user's personal system, but it also has the potential to pass that vulnerability on to Coast Guard systems through connections be they via the network or via transported disk. It is for this reason, that a user's personal computing habits must become of increasing import. In order to assess the scope of any vulnerability here, an organization must determine whether or not users are managing their personal systems in a safe manner.

d. Installing Software From Unknown Sources

On a properly configured Coast Guard Standard Workstation III, end users are prevented from installing software since they lack Windows NT administrator account privileges. If this protection were foolproof, it would appear that this would negate this as a security concern. However, installation prevention is not usually 100% effective, and, once again, user habits away from the office can affect Coast Guard systems here as well.

One of the largest concerns posed by the installation of software from unknown sources is the potential that such software might contain a Trojan Horse. Trojan Horse programs installed on personal systems would remain active if that system were remotely connected. When considered in conjunction with the password concerns above, Trojan Horse programs designed to capture passwords or keyboard input are especially dangerous since users might be using the same passwords on the Internet as they are for Coast Guard systems, and, in this case, any such password could be revealed as a result of the Trojan Horse.

Since the Coast Guard does not control the contents of users' personal systems, it is difficult to manage something of this nature. To mitigate the potential

vulnerability, users would have to be aware of the nature of such attacks and take care with regard to the items they installed on their personal systems.

2. Users' General Perceptions Regarding Systems and Policies

In any system with human interaction, user perceptions regarding to the need and working of that system are critical to its success. This is no less true of security programs and, in fact, these perceptions can prove even more critical since the costs associated with compromised systems tend to be significant. In order to minimize the risk of compromise, users would optimally possess a high awareness level with regard to security issues and would have a desire to ensure that secure practices were a high priority in the work place. User perceptions themselves are very hard to quantify, however, there can be some key indicators with regard to the general perception level. The actions of users and groups with respect to policy issues, the general knowledge and skill levels of the users, security awareness levels and the tendency of users to trust (or not trust) the system all form part of user perceptions, and each plays a role in system security.

a. Actions of Users and Groups with Respect to Policy Issues

In the Coast Guard, as with many military organizations, there is a rigid, formal environment that is intended to provide the framework for the behavior of its personnel. In the area of information security, this is equally true.

Extensive policy manuals define the expected practices of users at all levels. The number and size of the manuals relating to any one topic can be significant. Coast Guard policy covering information security can currently be found in The Automated Information Systems Security Manual, (COMDINST M5500.13A), The

Security Awareness, Training, and Education Program Manual (COMDINST M5528.1), The Standard Workstation Security Handbook (COMDINST 5500.17), and among many others, Standard Workstation III Operating System Standards (COMDINST 5230.2). Each of these instructions provides Coast Guard-wide policy. Such instructions are often supplemented by Area, District, and local guidance as well. Having such a wide range of documents, will users know where to find guidance regarding any security concerns they may have?

Publication and availability of security policy is not the only concern with regard to user perceptions. After an organization defines its goals with regard to its expectations of security, the next step is ensuring that those priorities are communicated to and incorporated by the system users. A user who perceives security issues as an after thought or who is unaware of the role security plays in the work place is less likely to follow secure procedures.

If users feel that security measures hinder them in the performance of their duties, they may be more inclined to develop methods that circumvent secure procedures. Rather than seeking guidance, users may develop "work around" solutions in order to allow them to perform activities. Evidence of weak security perceptions can often be evidenced by a user's practices with regard to many of the actions addressed previously under security practices. In addition, if users feel that there is no real need for security in the transactions they engage in, they may be less likely to place great emphasis upon adhering to those practices.

Such activities are not always limited to individual users either. In some cases, larger groups (sections, divisions, or commands) may develop procedures that

circumvent standard security procedures for the purpose of advancing what are often seen as more pressing business concerns. A clear example of this, previously experienced by the author, is the practice of password sharing. Groups often feel that the need to accomplish day-to-day business activities efficiently outweighs the need to do so in a secure manner. Group passwords, providing passwords to administrative personnel for emergency access, and password sharing are all contrary to password policies, however, these actions have been known to occur in order to ensure that normal business activities proceed unhindered. Practices such as this, where users consciously act to circumvent security measures, would clearly indicate security issues are not being perceived and practiced in the manner dictated by policy.

b. General Knowledge and Skill Level of Users

Information system knowledge and skills are critical to performance in the modern age. This necessity for these skills will only increase as our dependence upon systems continues to grow. Without the proper knowledge and skills necessary, it is not a reasonable expectation that the user will perform tasks correctly, and while the Coast Guard requires a user to go through practical and written tests prior to being trusted at the helm, the same user may find him or herself in command of a Standard Workstation after signing a document and being provided a username. While this may be the worst-case scenario, it is not unheard of, and all users do not approach their systems on equal footing.

One key concern in this regard is the level of computer skills required to perform one's duties. If a user doesn't possess at least this basic level, they cannot be expected to perform the tasks necessary of them correctly or without assistance. If,

however, the individual recognizes their own lower skill level, they may be inclined to ask for assistance from either coworkers or system administrators. In the first case, the user may not receive useful assistance if the users within the group are at an equal or lesser skill and knowledge level. In addition, if guidance is sought from users who routinely seek "work around" solutions, this only amplifies the potential for propagation of such techniques. If, on the other hand, users regularly seek the guidance of the system administrators, users may find that those personnel can quickly become overburdened.

Prior to 1995 the Coast Guard's Standard Workstation II utilized the BTOS and CTOS operating systems. Since there was no personal computing market for those systems, the service could operate fairly confidently under the assumption that users were gaining their knowledge and perceptions of system use while on the job. Since the Coast Guard has transferred to a Windows-based environment, this is no longer true.

Many of the Coast Guard's users today use their personal systems as much, if not more than their systems at work. Perceptions and practices developed through home use now carry over easily into the work environment. These perceptions can enhance security if users develop safe practices due to their desire to protect personal information, foster discontent if they perceive that security policies allow them to do things at home that are prevented at work, and even lead to less secure situations if they become accustomed to engaging in insecure practices outside work since these might in turn carry over to the work environment.

c. Security Awareness Level of Users

Properly gauging users' perceptions regarding the computer skill level they feel they possess versus the level they require to adequately perform their duties coupled with an assessment of the practices in which they routinely engage can provide valuable insight into potential areas of concern. This is especially important since users developing poor habits in these areas may not even be aware of the security implications of their actions. The threat this poses is clearly significant, and according to both Ernst & Young's Second Annual Global Information Security Survey [Ref. 11] and The Business Information Security Survey (BISS 2000) [Ref. 12], the lack of user-level security awareness is the largest obstacle to Information Security and proposed solutions.

The Automated Information Systems Security Manual, (COMDINST M5500.13A) [Ref. 13] defines security awareness as "a state of mind through which an individual is conscious of the existence of a security program and is persuaded that the program is relevant to his or her own behavior." The manual recognizes that there can be a relationship between awareness, knowledge, and training, but it clearly distinguishes between them, noting that, while intimately related, it is a "conscious process...which can move an individual to specific actions." Understanding that there is a need for information security awareness, the Coast Guard must determine what the awareness level of its users is. In attempting to raise awareness, it must also decide which measures will be best accepted by the user population, and which measures will prove to be the most effective in increasing awareness levels.

d. Trust in System Integrity

In every human exchange, there is an element of trust that occurs. Whether money or information is exchanged, the willingness of an individual to engage in the transaction is governed by tendencies of trust. In this regard, people extend their trust to both the other party to the transaction as well as to the transaction mechanism. If people trust both the other party and the mechanism, the transaction can take place. However, if the user doesn't trust either of these, the transaction may be placed in jeopardy. Likewise, if the user inappropriately trusts these elements when they should not, then the transaction may be compromised.

In the information age, this plays a critical element in the expansion of e-Commerce and e-Government and it directly relates to the information security pillars of availability, confidentiality, and integrity. If users fail to trust the systems they should, they may be reluctant to perform transactions. In effect, failing to ensure that systems can be trusted results in the perception of insecurity and an unwillingness to use them; a de facto lack of availability. On the other hand, misplaced trust can result in the compromise of data which can affect both the confidentiality and integrity pillars of information security.

Many computer attacks rely heavily on the ability of the attacker to gain the ill-placed trust of a user: malicious code spreading through e-mail is lent credence by appearing to come from a known sender; e-mail forgeries are designed to lead the user to believe the material based upon the trust they place in the apparent sender; and Internet transactions are conducted under the assumption that the data will only be shared between the sender and the receiver.

Examination of user practices and perceptions can help answer whether users can currently determine when it is appropriate to trust remote systems and users. Examining differences between trusted and untrusted practices can help determine what causes users to place their trust in a system, whether or not users are able to validate their perceptions regarding trust, and it can also help in assessing current and potential methods of conveying trust to the individual.

3. Interaction with the User Interface

Today's Graphical User Interfaces have helped to allow computers to be used in a variety of tasks with an equally-diverse user base. Ideally, systems are designed to be "user friendly" so that performed actions are intuitive to the user and the system response is supposed to be equally predictable by the user.

A number of concerns exist with respect to security and the user interface. Among these are:

1. Applications are not designed with security as their primary focus. Thus, security is added later as a "plug-in" or a menu feature which is supplemental to the application's primary purpose and "user friendliness" toward that primary purpose may actually aid in compromising security;
2. Security-oriented messages and "help" systems often provide information which appears cryptic and of no use to the average user;
3. Security features which are demonstrated through the use of icons, menu choices, etc... can be easily misconstrued or left unused if users are untrained or unaware of their purpose; and

4. If systems are designed to be used in the same manner for both secure and non-secure transactions, even trained and aware users may become conditioned to one method and inadvertently use it at the inappropriate time.

Failure of the interface to rectify these concerns can lead to system compromise, and since attackers are fully aware of these potential flaws, attacks can be designed to capitalize on these areas and users may operate insecurely based on their inability to gain access to timely, accurate, and understandable information. The extent to which interface issues affect security is interdependent with many of the preceding concerns including awareness, trust, and practices. Examination of some of the common Standard Workstation III interface security features can help assess users' current ability to use those features and the potential for compliance with new features which may be considered in the future.

Having identified these concern areas, data collection regarding user perceptions and practices must be collected. For the purpose of this study, the primary data source will be a survey of a variety of Coast Guard system users. Properly constructing the survey toward assessing the identified areas of concern while ensuring the comfort and honesty of the survey participant can be difficult. The next section of this chapter describes the logic used in developing the survey used in the course of this study.

C. SURVEY DEVELOPMENT AND ADMINISTRATION

As the primary means of assessment for this study, proper construction and administration of the survey are critical to obtaining usable results. The study's Appendix provides a copy of the final survey used in the course of this study.

Throughout the following section, the rationale behind the selection of the questions is discussed. Details regarding the survey's administration are included as well.

1. Question Selection

In order to collect statistical data, the survey begins by requesting basic information regarding the individual's unit and specialty. For the purpose of tracking individual forms while maintaining anonymity, each form is assigned a unique form identification number.

The comfort of the individual asking the questions is important, and therefore, questions of a technical nature, and those that appear to have a distinctly right or wrong answer are not presented early in this survey. Instead, questions of a general nature are used to acclimate the participant prior to addressing specific security issues.

In questions 1 through 4, users are asked to evaluate the skill and knowledge level of themselves and their peers in relation to their assigned duties. The 1 through 7 scale chosen for this survey is used for familiarity's sake since this is the same scale currently used for Coast Guard personnel evaluations.

Further addressing general activities of the user, questions 5 and 6 attempt to discern tendencies of users with regard to handling both routine and more difficult computer issues. Examples of each instance are given to aid users in determining the difference between "use questions" and "problems."

Questions 7 through 14 further begin a series of yes/no questions. Since these questions do not reflect directly upon activities under the user's control, but rather on policy issues, they are further designed to ease the participant into the survey. In addition, the questions attempt to illicit whether users have access to the material

necessary to find answers to questions and problems on their own, and whether they feel that those policies are followed.

Beginning with question 15 user-specific data is starting to be collected with regard to e-mail tendencies and practices. Several areas are addressed within this topic, including, the origination of e-mail, suspect e-mail, unofficial e-mail, and handling of attachments.

Questions 23 through 28 conclude this first section of yes/no questions by addressing specific practices, and determining whether the user has access to a computer system outside of the ones used at work.

Since some of the final questions in the previous section could have made the user uncomfortable, another general use question is used. Question 29 seeks to gain information regarding the familiarity of users with various software. Knowing which software is used by most users in the Coast Guard can help to target security awareness measures to be applied in the context of those applications. For instance, if the majority of users limit their system use to Microsoft Word and Microsoft Outlook, increased awareness of viruses spread through e-mail and macros could be sought.

For users with home systems, question 30 seeks to determine if users are managing operating system updates with any frequency. A failure in this area could raise security concerns with regard to remote access.

The entirety of pages 5 and 6 of the survey is dedicated to user practices and perceptions regarding passwords and system access. For comparison with other research, the number of user passwords is requested, and some questions attempt to define the

scope of some author-witnessed practices including large groups of users sharing a single password and work groups requiring that passwords be filed with administrative support staff personnel for "emergency" access.

Question 43 lists a number of password practices which increase the likelihood that a password could be easily "cracked" through malicious means. Since weak passwords are one of the most common and dangerous security deficiencies, knowing the probability that users are following weak password practices will aid in evaluating whether password mechanisms are currently sound and whether other techniques for user identification and authentication should be pursued.

Since password compromise could have potentially detrimental effects, it is critical for users to understand how to change their passwords if necessary. Question 41 is an attempt to determine whether or not users actually know how to change their passwords, and if the user doesn't know how, then their perceptions regarding how to handle the situation of a possible password compromise are sought.

Windows NT performs a number of tasks through the user of the "trusted path." The trusted path is designed to provide an assurance to the user that, for critical actions, the user is actual communicating with the operating system, and not a Trojan Horse program. In order to invoke the trusted path on a Windows NT based system, the user must press the Ctrl-Alt-Delete keyboard combination. Two of the common actions that require this are changing the user password, and logging onto the system. Users should be aware that there is malicious software designed to steal passwords, and some of the steps necessary to mitigate that risk. Question 45 attempts to discern whether or not users are aware that they should attempt to invoke the trusted path prior to a log on attempt (As

demonstrated by the screen shot used for this question, it is not difficult to create a visual basic program to simulate the Windows NT logon screen. In fact, it would have proved more difficult to obtain a screen shot prior to a valid logon to the system).

Since viruses pose such a significant threat, it is critical that users be able to identify those files which could at least potentially carry a virus. If users do not believe that a potentially dangerous file type can actually carry malicious code, the tendency to open an infected attachment could prove more likely.

To assist in determining the risk this poses, participants are asked to identify, from a list of 42 files, which, if any could potentially carry malicious code. Despite the fact that the default Windows setting hides the 3-letter file extension, this information is provided to participants to assist them in determining the whether or not the file can be infected. Included in the list are the many of the most common file types, the most frequently infected file types, and several suspicious-looking, yet benign files (including Chernobyl.AVI, I LUV YOU.BMP, and Trojan Italic.TTF).

Questions 47 through 53 present a number of "myths" to the participants via a series of "True or False" questions. The questions will aid in determining whether users are aware of how viruses spread and what differences they are likely to note with their systems.

Questions 54 through 57 are designed to assess the threat of users home systems being susceptible to infection. The currency of virus protection software, software installation/configuration management, and the familiarity of other users all influence the risk posed to users' home systems, and by extension, Coast Guard systems if materials are exchanged with work, or remote connections occur.

Hardware security is another significant aspect of security. Most users are not aware of the ease with which key logging equipment can be attached to a computer system. If users are unaware of such techniques, and are unfamiliar with the equipment they should expect to have present, the potential for the successful use of such items increases.

As organizations attempt to take advantage of new technologies, security features are developed and added to applications. How these solutions are integrated into the user interface and perceptions they create for users is critical to their successful use. One example stemming from the increased use of the Internet and the need to provide for secure transactions is the use of Secure Socket Layer (SSL) transactions for web browsers.

Questions 59 through 66 are designed to address several potential issues with current methods of providing secure Internet transactions. Participants are presented with screen images of two actual Internet sites which request personal information from the user. The sites were selected as samples of the type of information commonly exchanged on the Internet today. The first is a bank that provides Internet banking options, and the second is a commercial services web site that allows for Internet payment via credit card. One key difference, however, is the fact that the first site uses an SSL connection while the second site does not.

Participants are queried regarding their perceptions of the two sites to determine their willingness to provide information to the sites and their reasons behind whether or not they trust the sites. On the following page, participants are asked directly about the meaning of the closed padlock indicating an SSL connection.

clarification of any provided comments. To solidify assurances of confidentiality, participants were asked to remove the cover sheets and turn them in separately and were assured that those sheets would be destroyed upon the completion of analysis portion of the study. The cover sheets have since been destroyed, and there is no means of identifying any individual's response to the survey.

Upon completing the surveys, participants were thanked for their participation and provided with an e-mail address to contact the author as well as the opportunity to discuss the survey. The length of time required to complete the survey varied from 30 minutes to 65 minutes. Most participants spent approximately 40 minutes completing the survey.

D. OTHER METHODS OF ASSESSMENT

1. Discussions With System Users

As mentioned in the survey administration section, participants were offered the opportunity to openly discuss any issues they would like regarding information security policies and practices. Several discussions resulted in the author garnering additional comments and concerns regarding information security issues. In addition, the author also received a number of comments from Coast Guard system users who were not survey participants.

The author found the opportunity to interact with, interview, and discuss the relevant issues of this study with system users helpful in the development of the survey and as a source of additional information outside the scope of the survey's statistical results. Specific items brought to the author's attention from non-survey participants are identified as such within the results section of this study.

2. E-Mail-Based Practical Exercise

Since trust and e-mail form such a critical link for so many issues on the user side of information security, the author developed a practical exercise to test the ability of participants to discern the origin of an e-mail message. The exercise was based on a previous project conducted by the author.

In the previous project, the author, with the knowledge of the professor, constructed an e-mail message to the other 15 graduate-level students in the section, all of whom were pursuing degrees in information technology programs. The message was created using an MSN Hotmail account, but with the professor's name provided as the "display name." Since all e-mail addresses used were campus addresses, it was assumed that most, if not all, participants would receive the e-mail using the campus' default mail client, Microsoft Outlook.

The message sent to the students was intended to be an obvious spoof of one of the many e-mail hoaxes spreading over the Internet. The e-mail read as follows:

NPS and Microsoft have entered into a joint venture. In support of the Navy's decision to move to IT21, NPS and Microsoft have decided to offer a special promotion and are offering, for a limited time:

----FREE GRADES-----

For complete details regarding the requirements necessary, please attend Monday's 10:00 AM session of CS3030, or you may feel free to contact me at my extension 656-HOAX.

Respectfully,

[Name Used Withheld]
CDR, USN
Go Navy! Beat Army

Of the 15 students receiving the message, 3 replies were sent to the Hotmail account requesting further information regarding the program. Surprisingly, one student that replied to the e-mail and who happened to be absent for the presentation, subsequently approached the instructor stating, "I'm really interested in the free grades. I tried calling you at the extension, but I think it must be the wrong number."

In this case, the user interface aids in lending credibility to the message by showing only the "display name" in the user's e-mail in tray. If a user knows and trusts the individual they appear to be receiving the e-mail from, they are far less likely to check to confirm the properties of the actual e-mail address that aren't displayed until the e-mail is actually opened. In addition, other simple methods of e-mail forgery exist which allow for forging the e-mail address as well as the display name. This can even extend to the use of digital signatures since e-mail may be "digitally signed and verified" according to Outlook, but unless the user knows to click on the appropriate icon, they can't be sure whose signature the message was signed with.

To test the ability of Coast Guard users to determine whether an e-mail message actually originated from a Coast Guard sender, volunteers were selected from the pool of survey participants. Each participant received an introductory e-mail from the author explaining the purpose and requirements of the practical exercise as follows:

Subject: Computer Security Survey Participation

First I'd like to thank each of you, once again, for your assistance in completing the computer security awareness survey, but I'd also like to thank you for volunteering to participate in the following short e-mail exercise. This exercise will be a practical demonstration of skills involved with using your e-mail interface to identify valid and suspect e-mail items.

Shortly, you will receive 3 pieces of e-mail. Each of these will appear to originate from LT Shane Montoya who is currently serving at a Marine Safety

Office in Alaska. The subject lines of each of these e-mails will be simply "E-Mail A", "E-Mail B", and "E-Mail C".

Without consulting others and upon receiving the 3 e-mails, I'd like you to determine which of the e-mails (if any) come from a valid Coast Guard address and which (if any) is not valid. If you can't determine this, that's a perfectly acceptable answer as well. I'd also like you to give what you feel is an honest impression as to which if any of the e-mails you would have suspected (had you not been told specifically that you might receive a suspect e-mail...or if the person you received it from was familiar to you, (i.e. boss, coworker, etc...)) and why. (I've included a SAMPLE response below) Please forward your responses to tjwhalen@nps.navy.mil.

(The following are by no means correct...they are merely to serve as a sample for your responses)

E-Mail A Valid - LT Montoya is a great guy. I'd recognize his e-mail address anywhere.

E-Mail B Unknown - I can't tell. LT Montoya's e-mail doesn't ring a bell with me.

E-Mail C Invalid - It just looks fishy. I mean can somebody who went to college in Colorado really be in the Coast Guard?

I look forward to receiving your responses. If you have any questions regarding the survey, or its results upon completion of the analysis phase, I'd be happy to answer them.

Timothy J. Whalen
Information Technology Programs
Naval Postgraduate School
Monterey, CA 93943

Three e-mails were then sent to each of the participants. One of the E-mails was actually from LT Montoya in Alaska, and the other two were spoofed through different methods. In this case, the users were completely aware that they would probably be receiving e-mail that was not actually from a Coast Guard user. The purpose was to determine whether they would able to determine which of the e-mails was authentic and to gather their impressions as to whether or not they would have suspected and been able

to assess the validity of the messages if they had received them during the normal course of business.

E. CHAPTER CONCLUSION

Based upon data obtained from industry sources and other research, coupled with the author's own Coast Guard experience, a number of potential human factors-based information security concerns were identified. In order to assess the threat level posed by these concern areas, surveys and other methods of assessment were developed for the purpose of gauging the practices and perceptions of the user population.

In the next chapter, a detailed assessment of the collected data should provide evidence of the potential threat level that exists within the scope of the identified human factors concerns.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PRESENTATION AND ANALYSIS OF COLLECTED DATA

A. INTRODUCTION

In order to analyze the collected data, all survey responses were entered into database and spreadsheet tools. In this chapter, the resulting statistics as well as user comments and perceptions are discussed.

The chapter's initial section centers on the breakdown of the sample population with regard to both specialty and rank as well as the resultant handling of comparative results. Compiled data is then examined with regard to each of the potential areas of concern identified within Chapter II.

B. SAMPLE POPULATION BREAKDOWN

1. Analysis by Specialty

The sample selected for the purpose of this study was designed to obtain input from a variety of Coast Guard specialties. These included administrative, aviation, marine safety, vessel operations, and information technology specialties. Units were selected based upon availability, proximity, and their ability to provide personnel within the desired specialties. The number surveyed within each specialty is shown below in Figure 2.

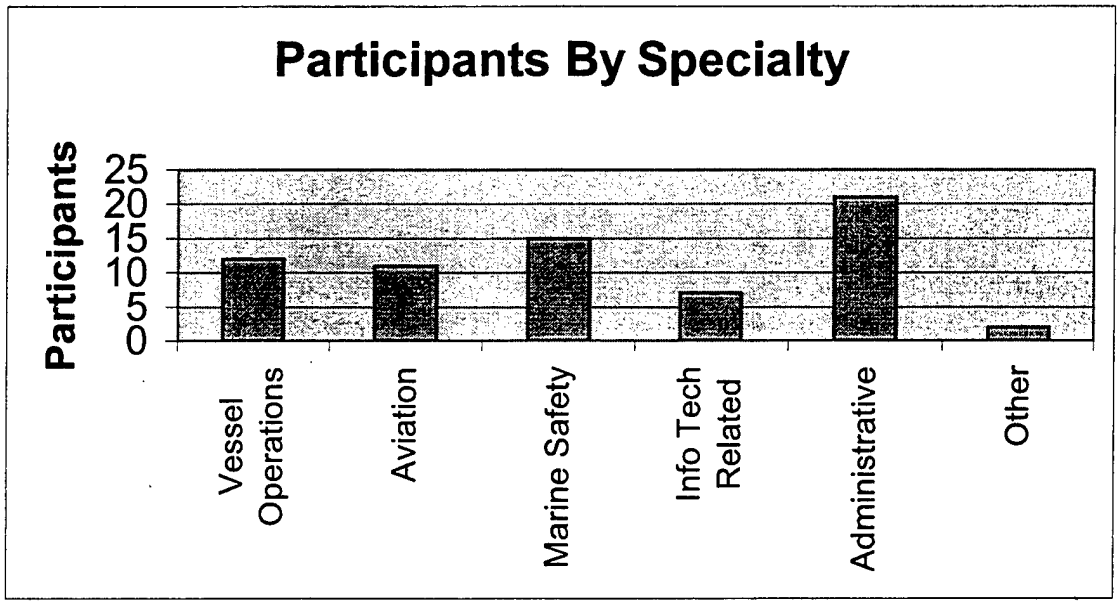


Figure 2. Surveyed Personnel By Specialty

Originally, the study intended to break down populations to further sub-specialties within the major categories, however, while 64 participants were available for the survey overall, the largest number available in any particular area was the 21 personnel within the administrative specialty. Further dividing each of the specialties would dilute results too much for consideration.

Four participants reported working within more than one specialty. These personnel had both an operational (marine safety, aviation, or vessel operations) and an additional specialty that was, in all cases, listed as either administrative or information technology related.

Since sample sizes were different for each of the communities, percentages were used in an attempt to provide comparison results. This method, while acceptable for noting large differences between samples, is not without problems associated with the smaller samples in some specialties. This becomes apparent when examining the

difference between those listing specialties of administrative and information technology related. A single unusual response in these categories would skew percentage results by approximately 5% and 15% respectively. For this reason, for each area of concern, the results of the overall sample population will be presented and larger differences will be noted if they appear significant.

2. Analysis by Grade

To ensure that a variety of experience levels and types were included, the sample population was also analyzed by category (i.e. officer, enlisted, or civilian) and grade to determine if all categories were represented. The breakdown of participants by grade is shown below in Figure 3. The results show that the grade of the participants varied greatly and significant numbers of enlisted, officer, and civilian personnel all took part in the study.

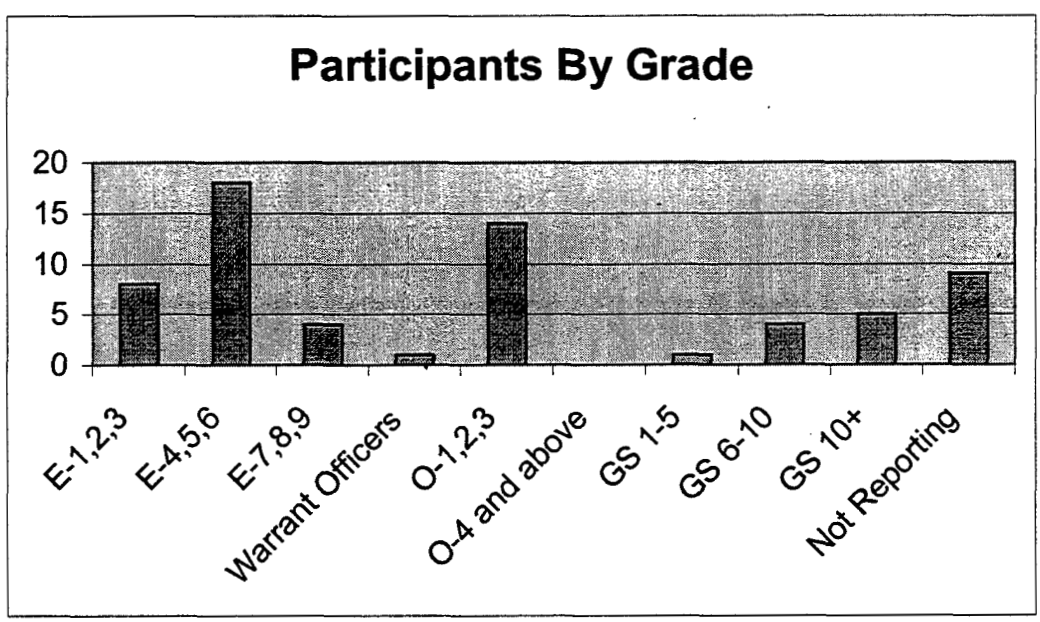


Figure 3. Surveyed Personnel By Grade

Noticeably absent among the participants are personnel in the grade of O-4 and above. While the lack of senior officer data and the specialty percentages do not map

directly to the Coast Guard's overall population proportions, it is believed that the survey will still provide data which can serve to indicate user tendencies, perceptions, and possible areas to focus improvement efforts.

C. ANALYSIS OF RESULTS

1. Evaluation of Skills

The 64 participants were first asked to evaluate their own computer skill levels as well as the skill level required to perform their duties. Participants provided this rating on a scale of 1 through 7. In comparing the two, 48% of the people surveyed felt that the skills necessary to complete their duties adequately exceeded their knowledge level. This is demonstrated graphically in Figure 4, below.

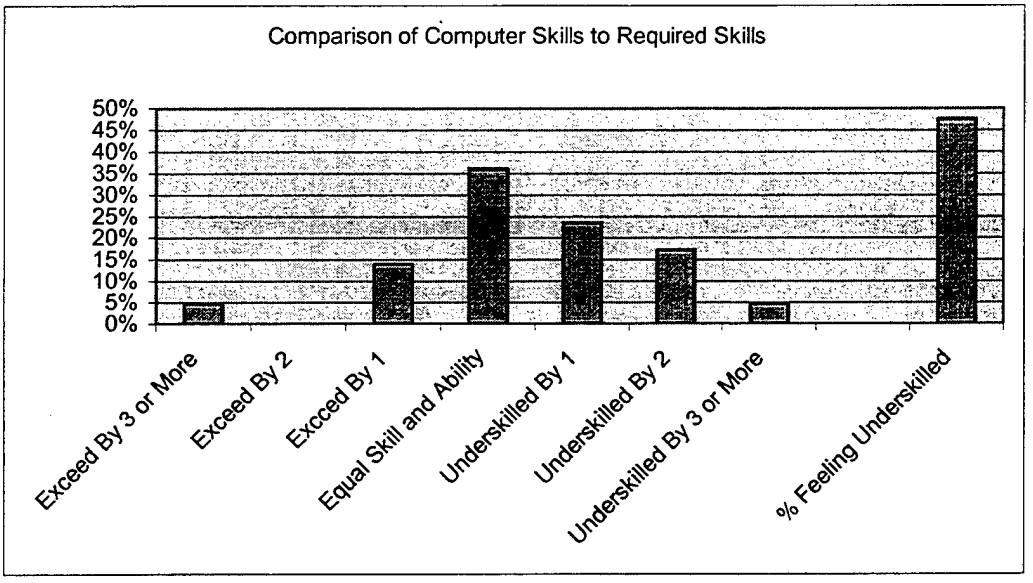


Figure 4. Comparison of Computer Skills to Required Skills.

A total of 19% of personnel felt that their abilities actually exceeded their duty requirements with 36% feeling that their skills met the level of their requirements. Statistically, participants also felt that their coworkers, on average, possessed a slightly

lower level of computer skills and most felt that their knowledge of computer security issues was less than that of their general computer knowledge.

The disparity between the participants' own skill level and that required to perform adequately demonstrates a need to increase those skill levels so that users are comfortable in the use of Coast Guard information systems. If users are not comfortable with their use of systems, or their knowledge of those systems, then the way they handle difficulties may prove to be unsatisfactory.

Figures 5 and 6 show how participants would handle situations where they are presented with general computer questions and with computer problems. The questions defined these two categories differently, with examples of each being provided.

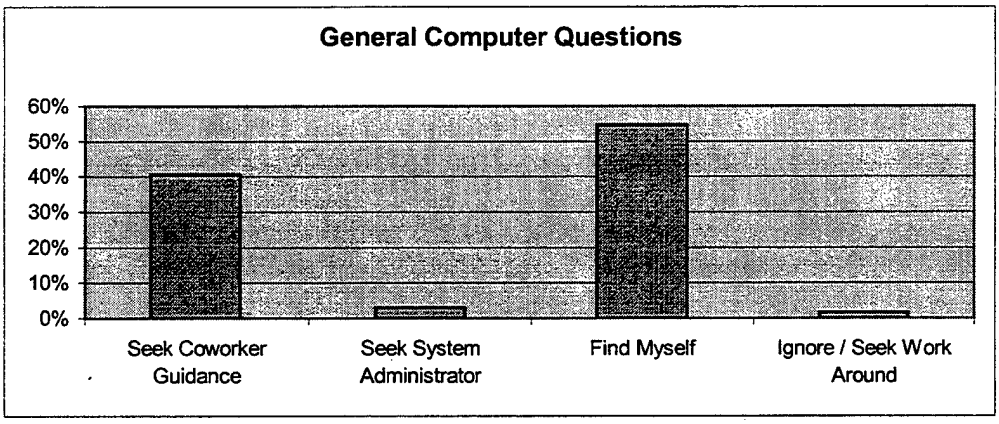


Figure 5. How Users Find Answers to General Computer Questions

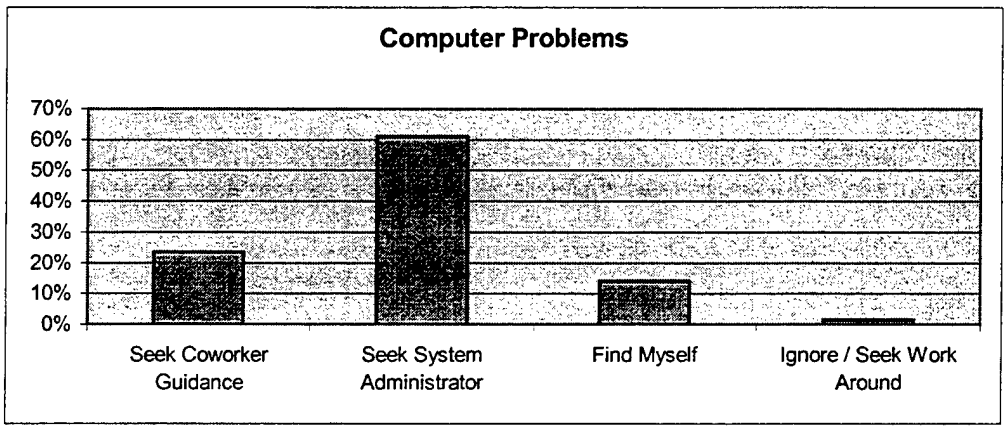


Figure 6. How Users Find Answers to Computer Problems

Most users prefer to find the answer to a general question themselves and would seek out the assistance of a system administrator in the case of an actual problem. In each case, the second most popular response indicated that seeking the guidance of a coworker was the participant's preferred option. While the tendency of users to attempt solutions on their own to seek the guidance of coworkers helps to relieve system administrators, it does not necessarily guarantee that the correct procedures are followed.

In order to proceed correctly, users faced with questions or problems would need to know where to find accurate information regarding the issue. This information comes from application user manuals, policy, and other sources. Figure 7, which will be referenced again later, provides some information as to whether users feel that they can reasonably find such information.

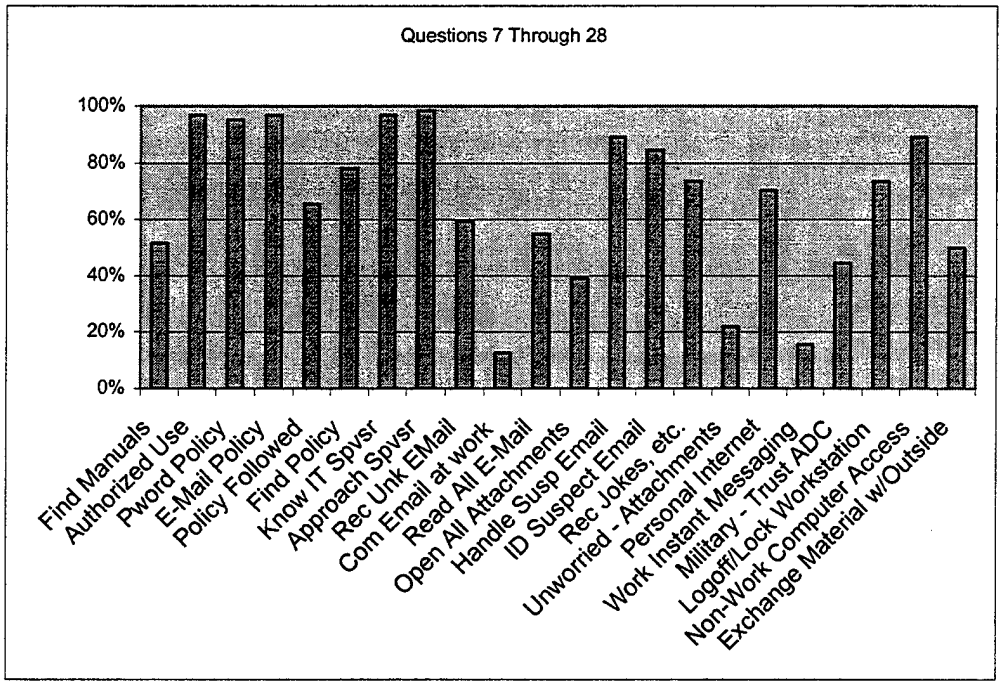


Figure 7. Participant Responses to Questions 7 Through 28

Just over half of all personnel felt that they knew the location of manuals for the software that they use. Without the ability to locate and use relevant manuals, a user's ability to find accurate information is limited and thus, so is the ability to adequately answer computer questions and problems through self-help. This is also true when users approach coworkers for assistance who are of a similar knowledge level.

These tendencies did not seem to vary greatly between the various user specialties, and while software manuals appear to be less available, more users seem to feel they know the policies regarding system use, feel they know where those policies are located and also feel comfortable in approaching the personnel supervising those policy issues. While these feelings sound encouraging, much of the data that follows is contraindicative of strong familiarity and adherence to those policies.

2. Use, Selection, and Changing of Passwords and Authentication Practices

Among the policy question responses shown graphically in Figure 7, 97% of the participants indicated that they were aware of the policy regarding authorized use. One of the primary methods of ensuring authorized use is through the use of authentication through passwords.

Overall, the average number of passwords held by an individual was about 6. This number varied by specialty from a low of 3.7 per participant in the vessel operations field to a high of 8.4 per user in the information technology field.

Approximately 45% of the participants indicated that the number of passwords they held exceeded the 5-password threshold identified in Ref. 6, and 20% of those surveyed indicated that the number of passwords they used was greater than 10. With a significant proportion of personnel and the majority of the specialties carrying large numbers of passwords, selection of those passwords becomes even more critical to ensuring authentication security measures.

Password selection, use, and policy all play key roles in the successful use of a password-based authentication mechanism. Questions 33 through 42 of the survey were designed gauge a number of these factors, and the results are shown in Figure 8, below.

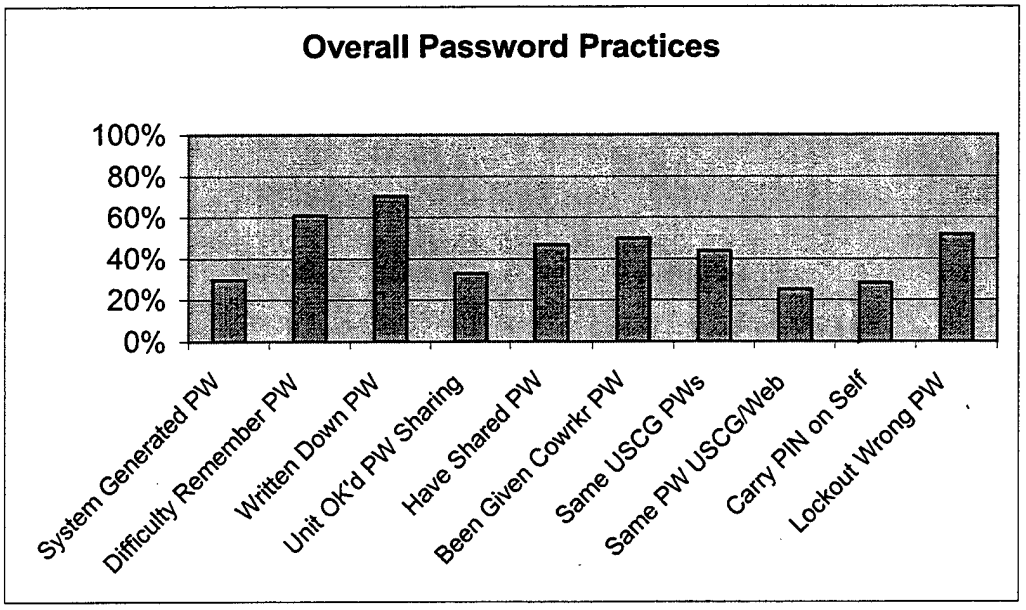


Figure 8. Participant Responses to Questions 33 Through 42

Well over half of all participants indicated that they sometimes have difficulty remembering passwords, and that has led to nearly half of them being locked out at some point or another for failing to supply the correct system password. 70% of the participants admitted that they have or do write their passwords down, however, many saw no problem or potential for compromise in doing so. One participant indicated that this was secure since the password was "...written down in one area no one will find," while another enters other passwords into a password-protected Palm Pilot.

Further queries to the database showed higher numbers of passwords for personnel with access to computers outside work than the 11 personnel who stated that they did not have access to a computer outside of work. With outside access increasing the number of passwords per system user further beyond the limits of the average person's ability to remember them, use of similar storage methods will most likely increase.

Password sharing is also a problem. Approximately half of the personnel admitted to sharing their passwords and a similar proportion stated that they've been given another's password for access as well. In addition, 1/3 of personnel indicated that their units have either condoned or "looked the other way" with regard to password sharing practices. These actions take place and appear to be commonplace despite the fact that 95% of the participants indicated that they knew the Coast Guard's policy regarding passwords and it lends credence to the "unmotivated user property" cited in Ref. 5. This states that "Security is usually a secondary goal...they want to send email, browse web pages, or download software, and they want security in place to protect them while they do those things." As such, if users feel that password measures provide roadblocks to their achieving normal working goals, they may feel the need to circumvent those measures.

The tendency to share passwords did appear to vary somewhat by specialty. The numbers ranged from a low of 25% among vessel operations personnel to a high of 80% among marine safety personnel. From the author's personnel experience, some of the tendency of marine safety workers to share passwords can be limited to MSIS, the primary database system used by marine safety personnel. Password sharing is almost routine for many users of this system. However, even if marine safety users are excluded based upon the possible skewing introduced from MSIS (which also forces users to use system-generated passwords, and which is currently being replaced), 25% - 45% of personnel would share their passwords, regardless of specialty, if current policies and perceptions remain.

Password sharing can facilitate compromise internally just as the construction and use of "weak" passwords can increase the likelihood that others could crack them. In order to assess Coast Guard user tendencies toward selecting weak or strong passwords, participants were asked to identify whether or not they used any of a number of practices that might weaken those passwords. On average, participants engaged in at least 3 password-weakening practices. The percentage of users utilizing each of these practices is identified below in Figure 9.

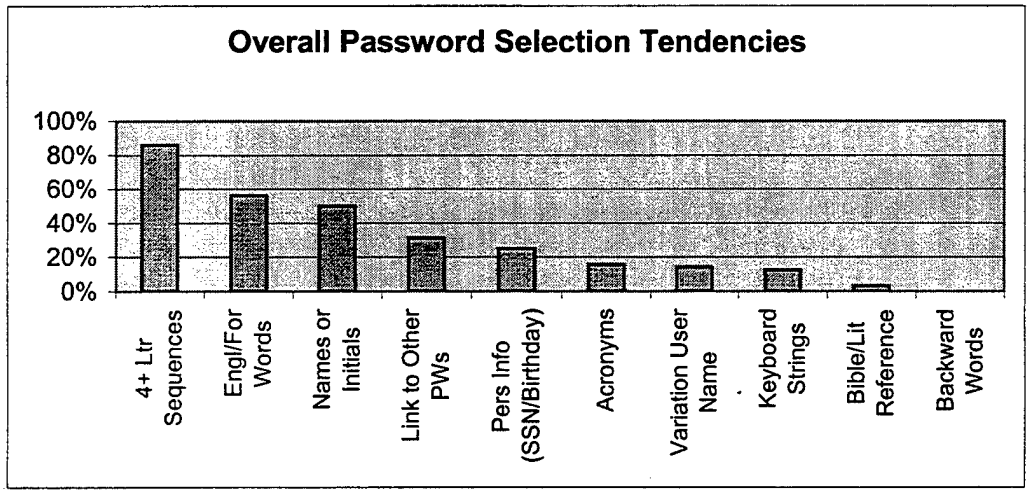


Figure 9. Password Selection Tendencies

There seemed to be no significant differences among the various specialties in terms of the number of selection practices used by the groups. Some individual practices did tend to have higher use rates by particular groups such as English and foreign words being used by 73% of marine safety personnel. However, other groups such as administrative personnel were more likely to select names or initials that can also weaken passwords. The risk posed by personnel using password-weakening practices to create their passwords increases when taken in conjunction with other factors such as those previously shown in Figure 7. Since 25% of participants admitted to using the same

passwords on both home and work systems, this increases the potential exposure of these weakened passwords.

Another means of possible compromise is through malicious attempts to capture a user's password as it is entered into the system. There are both software and hardware methods for doing this. In the case of software, Trojan horse programs designed to mimic logon screens as well as key logging software can be used to capture a user's password. Hardware solutions include special keyboards and wiring available over the Internet at relatively minimal costs. Whether or not Coast Guard users are susceptible to these attacks largely depends upon their awareness of them and whether or not they take the steps necessary to minimize the likelihood of their occurrence.

Question 45 asked participants how they would handle the Windows NT logon screen shown, assuming it was present as they approached the machine. In this case, a user should invoke the system's trusted path in an attempt to ensure that the program asking for the user name and password is in fact Windows NT. As shown in Figure 9, 94% of users did not feel the need invoke the system's trusted path, despite the fact that the key combination was listed as one of 5 possible choices.

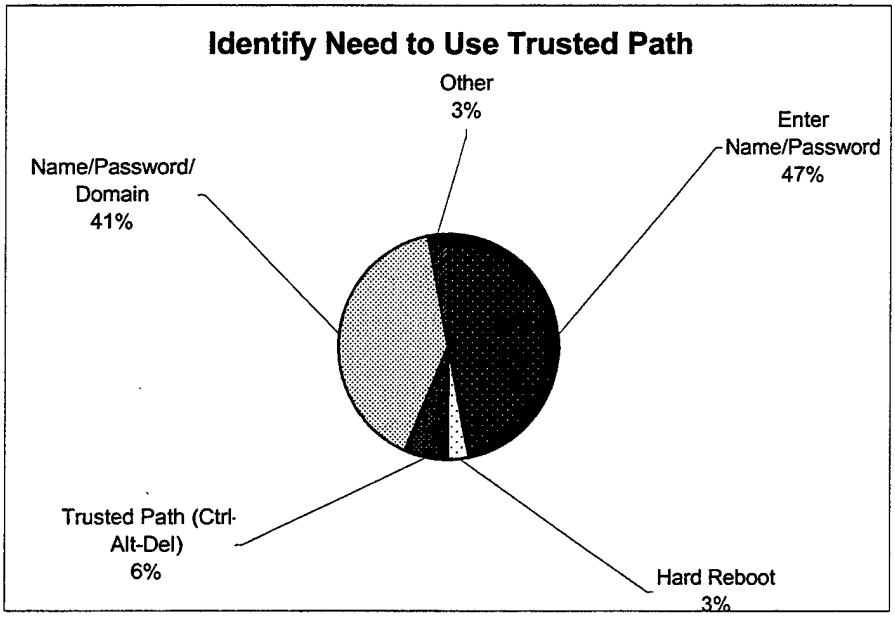


Figure 10. Tendency of Users to Invoke the Trusted Path

Based upon experience and conversations with users, it appears that many users have developed a tendency to press the Ctrl-Alt-Del key combination out of habit when approaching an idle workstation even if they are not aware that they are invoking the trusted path. This tendency develops from the need to perform this action to retrieve the logon screen if the machine has sat idle since the screensaver will have started in a properly configured workstation. While this might reduce the above results to some degree, it does not eliminate the lack of awareness of the purpose of the trusted path mechanism demonstrated in Figure 10.

The tendencies demonstrated with regard to password policy, selection, and practices indicates that system users do face a real threat of password compromise. For that reason, it is important that users understand the procedures necessary to change those passwords. This does not appear to be the case since only 27% of participants correctly knew how to change their own password in Windows NT. While an additional 35% of the participants stated that they would inform their system administrator, who could in

turn reset their password, this action would add an unnecessary delay to the process and might prove difficult since many users stated that they have difficulty finding a system administrator when they need them since they seem to have very full schedules already. The primary difference noted between specialties here was that two of the information systems workers were system managers who stated that they would change their own password by resetting it through NT's user manager function. While this practice would be relatively common for a system administrator, it is hoped that they would be able to inform users of the alternative, user-level means of resetting the password.

Aside from the software-based risks, hardware-based risks provide the potential for malicious activity as well. Internal risks of this technology abound as users could easily place the items, commercially available for as little as $139 [Ref. 14], on any system to which they have access. Once installed, they are undetectable through regular system use and are operating system independent. Figure 11 shows such an item attached to a system and demonstrates that even a trained user might easily overlook the item unless specifically looking for it.

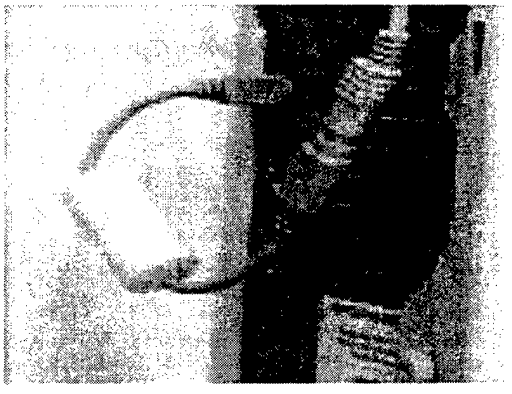


Figure 11. Sample of Hardware-Based Key Logger Attachment from: [Ref. 14]

Internally, these could be attached to a supervisor's (or other target's) system, attached to an attacker's own system prior to asking a system administrator for assistance.

As an external threat, any person with physical access to the system could attach the item whether these individuals are part of the janitorial crew, industry personnel, or others. The only true defense against such products would be an awareness of the threat combined with a regular check of the connections of each system used. Figure 12 seems to indicate that neither of these conditions currently exists.

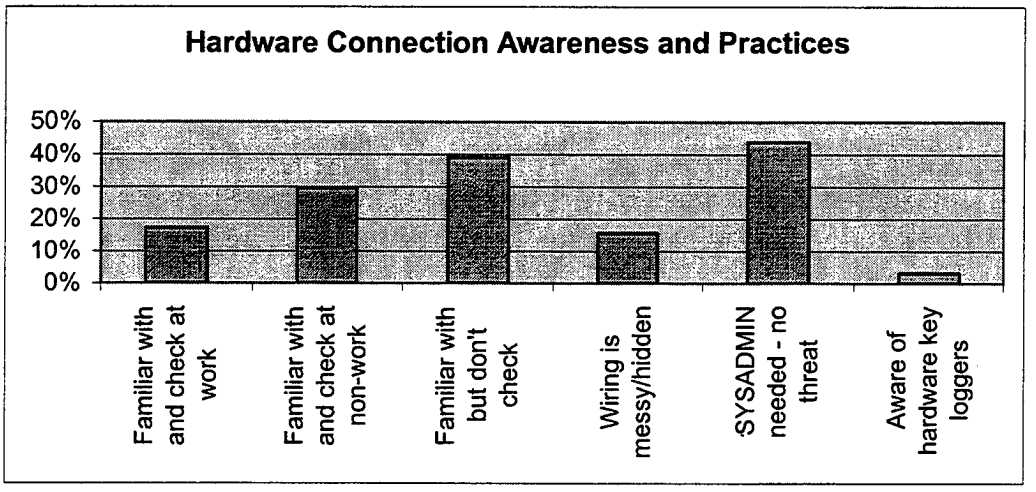


Figure 12. Hardware Connection Awareness and Practices

In this case, once again, there did not appear to be any major differences between the various user groups. Surprisingly, even 3 of the 7 (43%) of those with information technology related specialties felt that such items posed little threat and that they would have to be installed by a system administrator.

In general, it appears that password-use and authentication concerns present a strong potential threat to Coast Guard information security. Current policies are not strictly adhered to, users select weak passwords, and personal awareness of potential attack methods does not appear to be high. In addition, since the number of passwords per individual can probably be expected to increase as use of the Internet continues to grow, measures to mitigate this threat need to be examined. Plans within the military to

incorporate smart cards do not completely eliminate risks associated with such measures. Providing users with a smart card as the primary means of authentication merely substitutes physical security concerns for those of the password security concerns, and safeguarding such a card with a password or PIN reintroduces the original factors. In addition, designers of such programs should be fully aware that many personnel currently carry their bank ATM card PIN on their person. In the case of the participants of this study, 28% (see Figure 7) of the personnel surveyed did so, and it is reasonable to assume that a similar percentage would follow that practice should any smart card solution require the use of a password or PIN.

Analysis of password and authentication practices shows that the Coast Guard is not immune to the concerns raised by industry and the cited studies, and increased awareness measures appear necessary. In the next section, the study considers the susceptibility of Coast Guard users to suspect e-mail attachments and malicious code to determine whether this too falls in line with the level of concern found in industry.

3. Susceptibility to Suspect E-Mail Attachments and Malicious Code

E-mail has rapidly become a primary means of communication within both the government and business communities. Fast and efficient, it makes the transfer of documents and data simple to the average user. Unfortunately, this same ease of use has also allowed malicious users to easily spread malicious code, making e-mail-spread viruses the most-common form of virus infection.

Critical to a successful virus attack are several issues, including: the operating system used; the software used; and the user's awareness and actions. Figure 13 shows that the vast majority of Coast Guard system users are exposed to the Windows

environment and their system use includes standard office productivity applications including word processing, web browsing, e-mail, and spreadsheets. Coast Guard specific applications were also used by a majority of system users, but all other applications were used by less than half of the participants. While there are distinct differences between groups with regard to use of some of the less-used applications (such as FTP and other operating systems which were used by a higher percentage of personnel in information technology related specialties), the greatest threat for the spread of malicious code through the Coast Guard's NT-based infrastructure is through that common operating system thread combined with the high percentage of use of standard Microsoft Office applications.

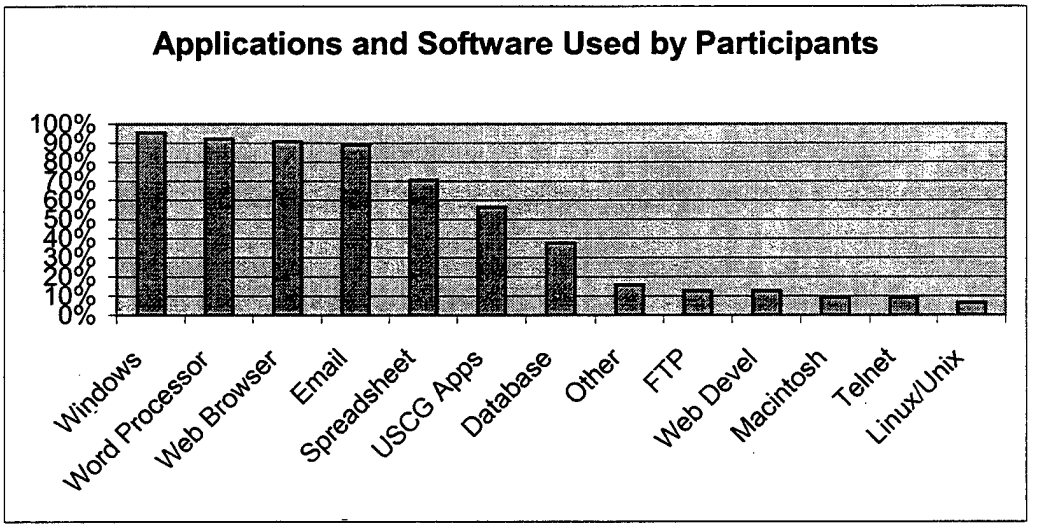


Figure 13. Applications and Software Used By Participants

With those points in common among nearly all system users (variation among applications occurred predominantly in the lesser-used applications), user awareness and practices become the greatest single threat for allowing the continued propagation of malicious code through e-mail and other delivery methods.

For that reason, user perceptions and capabilities are critical to minimizing the potential for these attacks. In the current use environment and in order to prevent a successful attack, users must be reasonably trusted to perform certain actions including properly determining the origin of e-mail, determining whether they trust the source of the message, and identifying objects which potentially carry malicious code. The problem is that most users don't appear to have these skills. Figure 14 provides information regarding the surveyed participants' ability to identify some of the more common files that are used to carry malicious code.

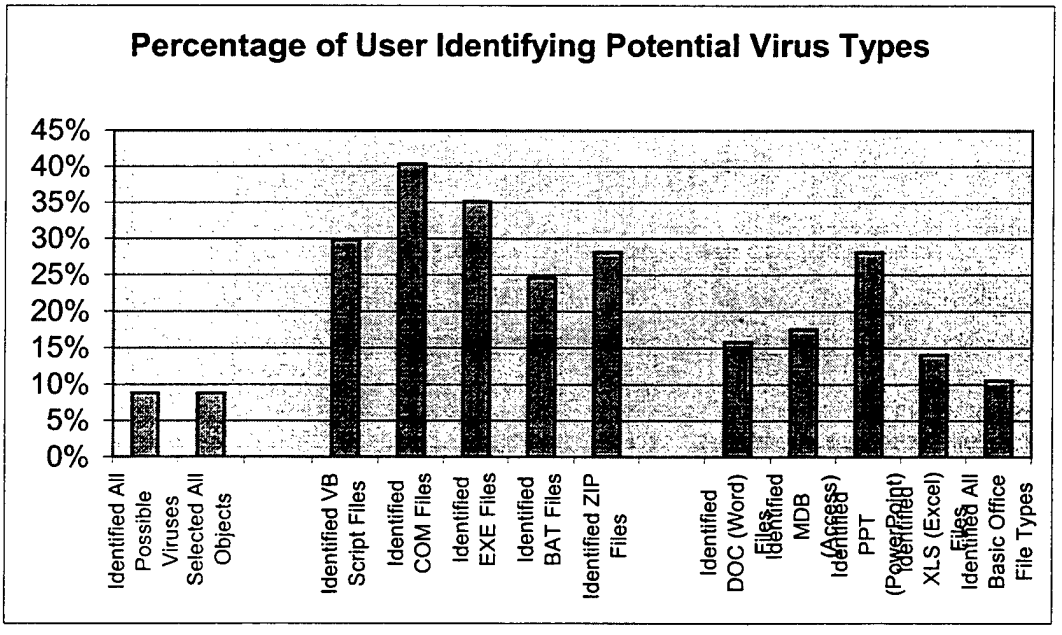


Figure 14. Percentage of Participants Identifying Potential Malicious Code Carriers

Despite the fact that most participants stated that they use Microsoft Office products and that the Coast Guard has issued guidance regarding macro viruses for these applications, the majority of users failed to recognize that these files could carry malicious code. In addition, 70% users failed to recognize Visual Basic Script (VBS) files as potentially harmful.

The percentage figures indicated by Figure 14 could even be perceived as being artificially high. This is because the 9% of users who circled the entire list of files are included in this breakdown. In addition, the percentage of users capable of identifying potentially harmful file types, once again, was not significantly impacted by the participant's specialty. In fact, aside from those selecting all possible file types, only one participant correctly selected VBS, COM, EXE, BAT, and ZIP files as being potentially harmful, and even this user failed to identify the threat posed by Office macro viruses.

While proceeding with the assumption that all files are potential carriers can lead to a safer environment, it may also prevent users from accessing valuable information. The author has personal experience with how this can prove to be extremely inconvenient. Installing Microsoft's Outlook Security patch prevents [Ref. 15] users from opening certain e-mail attachments including VBS, COM, EXE, BAT, and MDB files from those listed in Figure 14. By over-filtering and preventing users from exercising any judgment regarding the file attachments, the security update excludes large numbers of legitimate files as well. In the author's case, this prevented the exchange of EXE and Access database files that were both safe and needed to accomplish work. The use of the security update prevented the exchange of these files via the author's normal e-mail account.

When users apply blanket solutions, such as mistrusting all attachments out of fear or misunderstanding, they limit their own capabilities to fully capitalize on the systems they are using. When organizations react in this manner, they limit the capabilities of all users. Such solutions need to be carefully considered before they are applied to prevent user frustration and expanded use of user workarounds.

Other user perceptions with regard to viruses also play key roles in the ability of malicious code to spread. To determine whether system users knew the difference between malicious code facts and some common misperceptions, participants were asked a series of 7 true or false questions. User perceptions regarding these issues are represented in Figure 15.

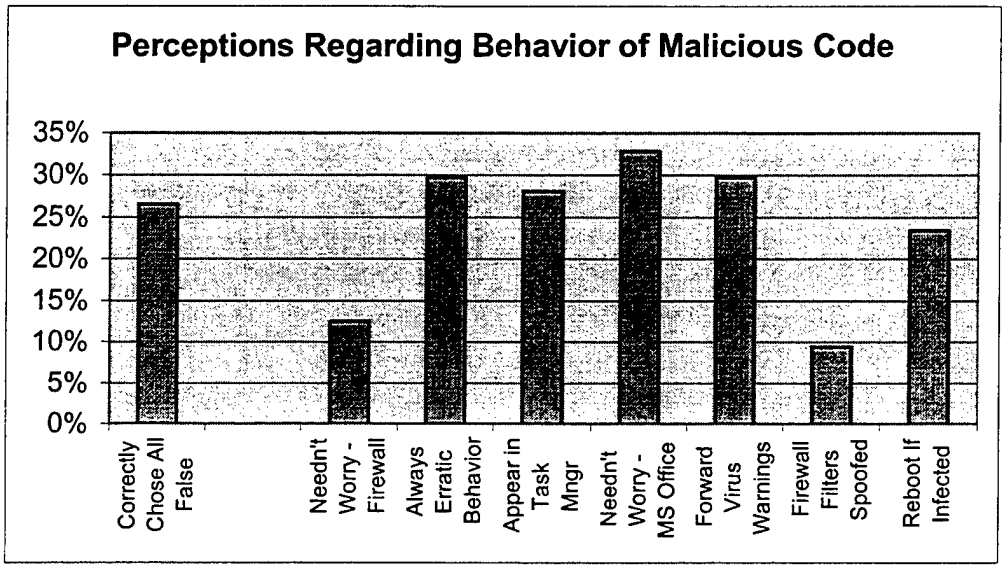


Figure 15. User Perceptions Regarding the Behavior of Malicious Code

Only 25% the participants correctly answered all questions as false, and no particular specialty, including those of the information technology related specialties, seemed to be able to have significantly better perceptions in this area.

Several of the questions seem to indicate that a significant number of users feel a false sense of security in that they feel the Coast Guard's firewall has capabilities that are unavailable, that malicious code infection is always obvious, and that limiting use to Microsoft Office products decreases the risk of infection. Increasing awareness of these and similar issues is critical if security decisions continue to fall into the hands of end

users. Since, as mentioned above, removing these decisions often leads to unacceptable restraints, the need for this increase is heightened.

Further problems are evidenced when users perceive that they are engaging in a secure action but are, in fact, compromising security. A clear example of this would be a user's tendency to determine the validity of a suspect e-mail message.

The brief e-mail exercise conducted as part of this study demonstrates that users cannot successfully complete actions they feel they know how to perform. Seven of the 10 participants who volunteered for and responded to the exercise, were unable to correctly determine whether each of the 3 e-mail messages actually came from a Coast Guard e-mail account. This occurred despite the fact that 84% of all participants stated that they felt that they could identify suspicious e-mail. (Direct correlation to the responding participants was not possible due to the anonymity measures taken. At the time responses were received, the cover sheets had already been destroyed.)

The results of the e-mail exercise are not necessarily surprising when compared to the results of the initial e-mail mentioned at the end of Chapter II. The Microsoft Outlook user interface actually assists in misleading users to trust fraudulent e-mail based upon its use of the "display name" in the user's In Tray. Figure 16 demonstrates that each of the 3 e-mails, appearing within the In Tray, seem to have been sent by LT Shane Montoya.

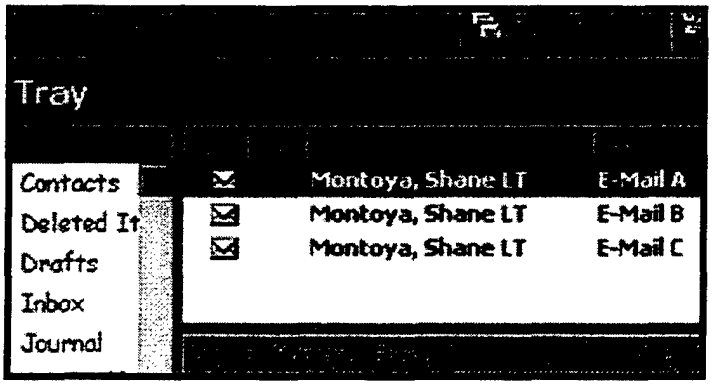


Figure 16. Graphical Display of Outlook In Tray

From the In Tray display alone, none of the e-mail messages appears suspicious. Figure 7 shows that most users open and read all e-mail they receive. Figure 17 shows that merely opening "E-Mail A" provides an indication that the e-mail is not from a Coast Guard user since the true originating e-mail address is displayed after the arbitrary display name. For this reason, 8 of the 10 participants were able to correctly identify e-mail "A" as suspect.

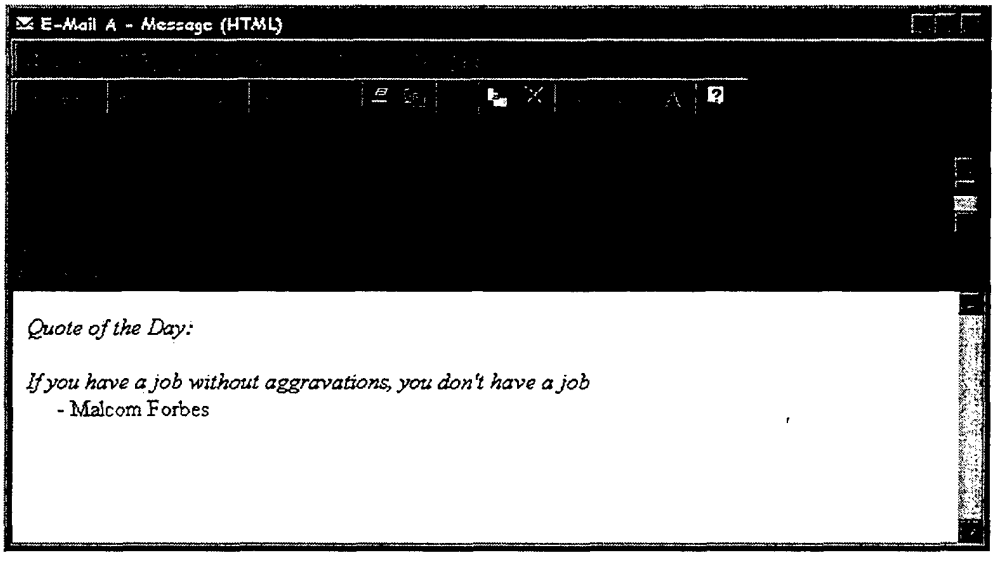


Figure 17. Hotmail Account Spoof of Display Name Only

The task became more difficult when users were asked to make determinations with regard to e-mails "B" (authentic) and "C" (forged). In order to make an assessment

of this e-mail, users had to be able to display the message's extended headers. Performing this action tends to be different for most e-mail client software packages and has even changed between the most recent versions of Outlook (98 and 2000). In addition, users would have to be able to actually interpret the information contained in those headers. Most participants were unable to do so. The user interface did not make these tasks easy. In fact, some people mistrusted the valid e-mail instead of the forged e-mail based upon information they did find provided to the by the user interface. In one case this was because the participant had brought up the properties feature associated with the e-mail address. Doing so, the participant found the e-mail address as Smontoya@cgalaska.uscg.mil. While this address is valid, it did not meet the participant's expectations since Alaskan units do not follow the @dXX.uscg.mil naming convention (where XX is the district number) established for most of the Coast Guard e-mail addresses.

The study also considered another area that is important to the prevention of virus infections. Properly installed and maintained, virus protection software can greatly assist in reducing the risks posed by virus infections. However, virus protection software which does not include recent virus definitions can prove worthless in these days of rapidly-spreading, new viruses. Figure 18 shows how participants responded with respect to virus protection software.

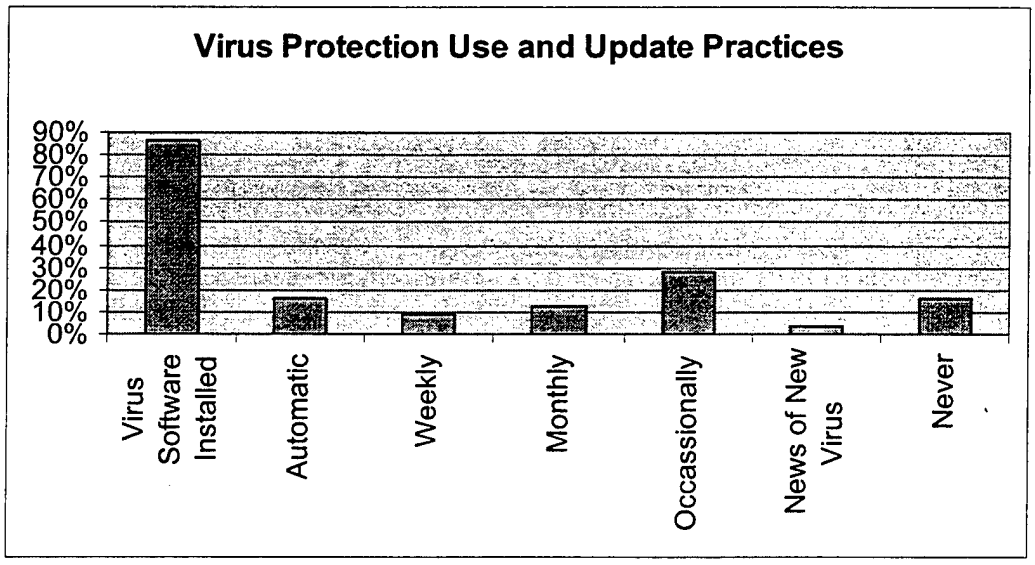


Figure 18. Virus Protection Update Practices

While 88% of those with outside computer access indicated that they had virus protection software installed, 60% of those same users updated that software monthly or less frequently, with 30 days being the maximum length of time between updates recommended by most virus protection software vendors. In addition, of the users stating that their software was set to manually update, none of those responding appeared to have taken all the necessary measures to ensure that connections could proceed completely automatically as discussed in Chapter II.

The failure of users to maintain virus definitions in an up-to-date manner could prove harmful to Coast Guard systems both with the expected increase in remote access and when considered with the Figure 7's data which shows that half of all the participants currently exchange material between work and their outside systems.

Actions on home systems may continue to pose increased threats with the expansion of remote access since software installation, operating system updates, and other similar actions are not subject to more stringent control measures as they are at

within the workplace. The next section will address potential areas of concern with regard to such practices outside the workplace.

4. Software Maintenance and Installation From Unknown Sources

When remote connections are allowed to outside systems, the Coast Guard's network security drops to the level of that system. Just as with virus protection software, the Coast Guard must rely on end users to ensure that appropriate software security patches are in place and that the software installed on those systems is trustworthy. However, as Figure 19 demonstrates, the participants themselves did not completely control the systems used outside of work with over half reporting that multiple people regularly install software on those non-work systems. This tendency will most probably become more prevalent as multiple-computer families, broadband access, and home networks continue to gain in popularity. Still, the installation of software by multiple people doesn't necessarily indicate that such software is from untrustworthy sources. However, 28% of the participants stated that it was normal for persons less familiar with computers than themselves to regularly install software. Since previous data presented has demonstrated that the surveyed users could find themselves susceptible to inadvertently executing malicious code through misplaced trust, it can be assumed that those less familiar users might be just as likely to perform those actions.

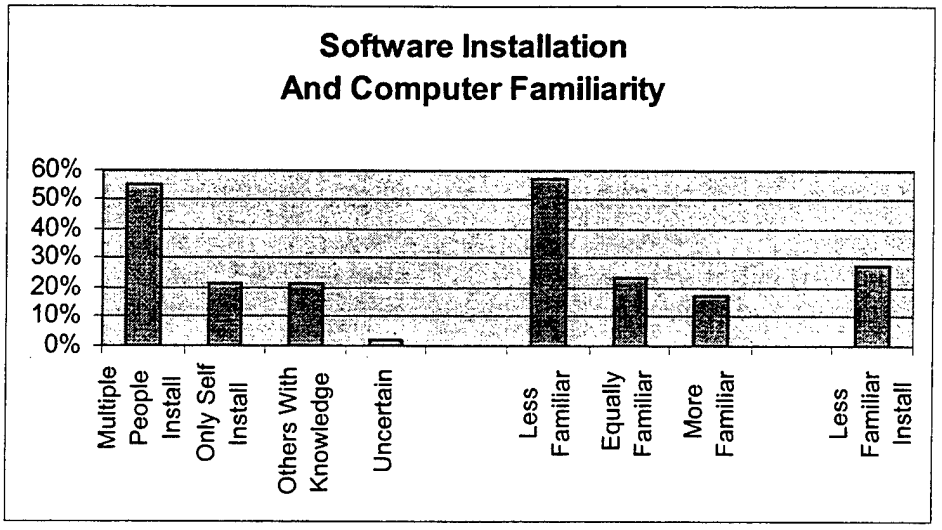


Figure 19. Software Installation and Computer Familiarity

With the exception of those working within information technology related specialties, there was very little difference between specialties with regard to the installation of software. In the case of the information technology workers, the only significant difference noted was that 100% of the personnel felt that the other users of their outside systems were less familiar with the systems than they were. This would be consistent with the fact that these personnel work professionally within that field. However, an important note is that information systems workers were just as likely as other groups to have others, all of whom were less familiar, installing software on their systems.

In addition to concerns regarding the applications installed on end-user systems, the updates to the operating system itself plays a key role in system security. Microsoft seems to routinely issue software security patches for its operating systems. The same is true for many Windows-based applications as well. Unfortunately, as Figure 20 shows, the vast majority of users fail to regularly check for and install updates, despite the fact

that most users utilize Windows-based operating systems that incorporate semi-automatic update features through "Windows Update."

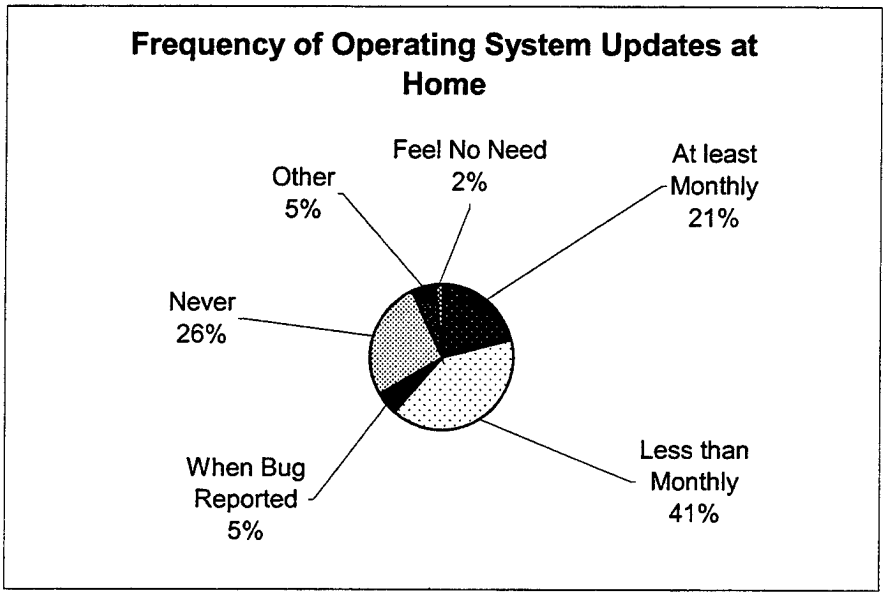


Figure 20. Frequency of Operating System Updates at Home

While users may feel secure in using their home systems and networks when they have failed to install recent updates, the Coast Guard needs to consider such trends when weighing the costs and benefits of remote access expansion.

While expansion of remote network connections could provide increased exposure to viral and update installation issues, the increased use of the Internet generates additional concerns as well. In the next section, the study's analysis examines users perceptions with regard to their use of secure Internet connections and the implications it might have on the increased use of such technologies.

5. Secure Socket Layer Transactions and Internet Trust

Currently, the primary means of providing secure transactions over the Internet is through the use of Secure Socket Layer (SSL) connections. This technology is currently

used by banking, commercial enterprise, and government sites to provide a secure connection between a system and remote user through the use of digital certificates.

Without such measures, transactions over the Internet would be subject to packet sniffing and other attacks which could compromise the data during transmission. For this reason, it is important that if users don't have an understanding of how the technology works, that they at least have an awareness of the indications that a secure connection is in fact in place. It is also important that users feel that they can trust the security of those transactions and that they be able to assess messages returned by the system. Figure 21 provides information regarding the participant's perceptions regarding two web sites presented to them as part of the survey.

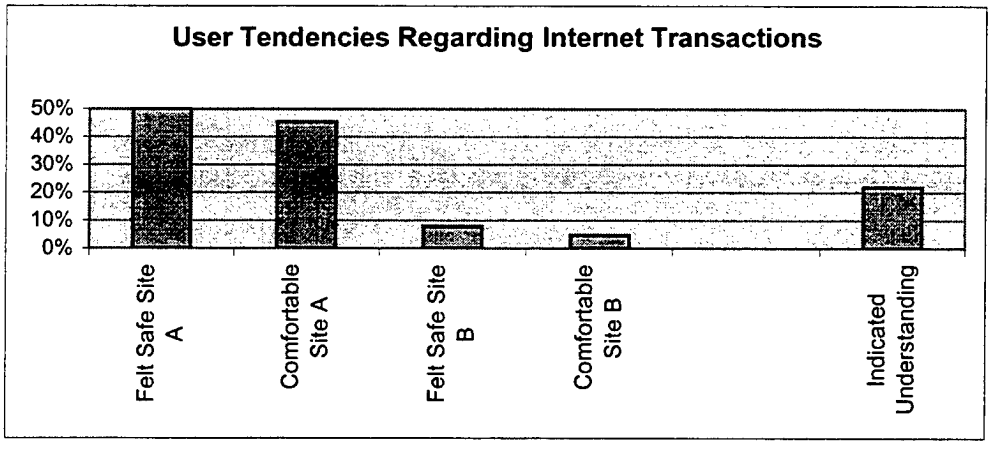


Figure 21. User Tendencies Regarding Internet Transactions

Site "A" was a major commercial banking institution that uses SSL to ensure the security of its transactions. Site "B" was a purebred dog registration site that requested credit card payment over the Internet for its registration services. This site does not use an SSL connection to protect this information.

While only about half of all personnel felt safe and comfortable conducting transactions on the Internet, it appeared, at first, that those who did recognized the security provided them by the SSL connection. The follow on question, however, indicated otherwise. User comments indicated that most users did not know about or understand the security measures used by Site "A." Instead, users tended to trust the site for a number of collateral reasons including the fact that it appeared to be more professionally presented, that they recognized the bank and its reputation, and that they may have accessed their own bank accounts through similar sites. On the other hand, participant reluctance to use site "B" was largely due to similar reasons including poor color schemes. In most cases, participants were more reluctant to provide credit card numbers than to merely access account information, but the opposite was true as well, with one user noting that credit card "...liability is limited to $35.00," while exposing bank account information could lead to a much greater loss.

On the following page, users were specifically asked the purpose of the SSL-indicating padlock icon displayed on site "A." When specifically asked about this, 63% of the participants understood that this was supposed to provide them with some indication that the site had a secure connection. This understanding did not vary greatly across the various specialties with information systems workers obtaining the highest rate of 71%. However, user comments, combined with the lower feelings of trust and safety indicate that what they are told is secure does not necessarily inspire trust.

User comments regarding the follow-on screen images also communicated discouragement among the participants. Many felt that the warnings, notices, and "help" screens were cryptic and confusing. A common answer for many participants was "?"

indicating that participants had no idea what they were being told. Furthermore, when users didn't understand what they were being told, their tendency to trust the site and willingness to perform transactions there dropped significantly.

This, combined with the data shown in the e-mail exercise clearly demonstrates that the user interface is critical to the formation of user perceptions, whether positive or negative, that influence user trust. These user expectations and assumptions can greatly impact security programs and are critical to successfully providing secure computing services in the future.

D. CHAPTER CONCLUSION

In this chapter, the study analyzed the data obtained in the survey and identified several potential security threats to the Coast Guard's information infrastructure. As the organization and the government as a whole proceed to further develop information technologies, secure transactions will continue to increase in frequency of use and import.

In order to ensure that users securely interact with those systems, the Coast Guard will need to take steps to increase user awareness and develop systems that the users can be reasonably expected to properly and securely use, but what are the right steps to take toward this goal? The next chapter will attempt to analyze some possible alternatives and make recommendations to assist in maintaining both information technology growth and a secure computing environment.

IV. CONCLUSION AND RECOMMENDATIONS

A. SUMMARY OF DATA ANALYSIS

Based upon the findings reported in Chapter II, it is apparent that human-factors-based security concerns present in the industry and identified in other bodies of research are equally prevalent within the United States Coast Guard. System user weaknesses were identified in each of the evaluated potential areas of concern, and reduction of these tendencies does not appear to relate directly to the experience level of the user. If it did, those users in the information technology field would have been expected to fare dramatically better, but this was not the case. While that user group did demonstrate differing ability levels in some areas, they were by no means immune to many of the common practices and perceptions that formed the weaknesses identified in the general sample population.

Since information technology personnel seemed to share many of the same weaknesses as the general population, it appears that experience alone does not necessarily eliminate security concerns. So, what measures can the Coast Guard take to reduce the occurrence of insecure practices? In the next section, the study will discuss possible alternatives that could be implemented to reduce the level of concern.

B. PRACTICE IMPROVEMENT MEASURES

1. User Authentication

Since the data collected in this study supports the conclusions reached by Adams and Sasse [Ref. 6] and demonstrates that many of their concerns are common among Coast Guard users, a number of their recommendations could also prove valuable in mitigating the potential security concerns for the Coast Guard. Among the

recommendations that might prove useful are the utilization of smart cards, biometrics, and a single sign on, in addition to increased user awareness. Each of these recommendations has the potential to assist in alleviating some of the concerns identified in the course of this study and they are discussed individually, below.

a. Smart Cards

Smart cards provide strong potential for reducing the number of passwords used by system users at work. In doing so, as mentioned in Chapter III, they substitute physical security concerns for the password concerns they would be used to replace. That being the case, implementation of any such program would rest heavily on the ability of users to secure their smart cards and loss rates would probably be similar to those currently found for identification cards.

In the case of a military identification card, the individual's photograph and signature on the card provide an additional level of security to prevent unauthorized use. In the case of a smart card, additional security could be attained through the use of a password or PIN, but also as stated in Chapter III, a significant number of users currently carry PIN's on their person with their bankcards. Without strong awareness, a similar number of users might be inclined to carry smart card PIN's as well.

Whether or not users are comfortable using such technology is an additional hurdle for program implementation. Survey results indicated that only 45% of personnel felt comfortable with using smart cards, however, through comments several of the participants indicated that they would probably feel comfortable if they were trained in their proper use.

b. Biometric Devices

Biometric devices provide an additional means of secure authentication that removes the normal physical security concerns of loss and theft one faces with the use of smart cards. Finger print scanners, optical scanners, and similar devices establish a user's identity that can be used for access.

Due to the physical nature of these devices, some users feel less comfortable using them, however, the survey showed that 55% of the participants were willing to utilize these devices vs. the 45% who were willing to use smart cards. Further examination showed that those working in information technology related fields, since all 7 of these individuals felt comfortable using such devices, somewhat skewed these results. However, once again, personnel indicated a willingness to use such technology with training in its proper use.

c. Single Sign On

Both smart cards and biometrics have significant disadvantage to users in that additional hardware is required to support such devices. The cost and availability of these hardware components might prevent users from being able to use these technologies and simultaneously take advantage of opportunities for telecommuting and expanded use of remote access. Without the use of additional hardware, single sign on can be used to relieve many authentication concerns while still allowing users the flexibility of remote access and without a significant hardware investment.

Single sign on eliminates the need for multiple passwords on work systems. With the system set to allow predetermined access levels to each application used, users are able to complete their duties and they are not forced into developing

elaborate means to store or remember an increasing list of passwords. However, such a solution may introduce a management burden a may not be flexible because of that.

While single sign on might alleviate some problems, it would not eliminate them. Development efforts undertaken in this direction would have to take into consideration the need of users to access non-Coast Guard systems such as those within the Department of Defense and other federal agencies to determine whether access to those systems could be supported as well. In addition, the tendency of users to select the same passwords at home and at work remains a concern and, in fact, the risk posed by a single breach would be greater since access to all systems would then rely upon a single point of failure.

d. Increased User Awareness

A common element of each of the previous, potential methods of improvement is increased user awareness. Whether the Coast Guard continues to use its current system or attempts to implement any of the three previous technologies, competent and willing participation by users is critical to successful efforts to provide system security. Finally, when dealing with hardware-based key logging attacks, user awareness and actions appear to be the only current way available to identify and handle these threats.

Perfectly outlined security policies and procedures are of little benefit if users and organizations are unaware of their requirements or do not follow them, just as users cannot be expected to create strong passwords or change those passwords if they are unaware of how to do so.

2. E-Mail Security and Execution of Malicious Code

Most recent virus outbreaks have propagated the use of e-mail attachments. In order to prevent the spread of such viruses, the ability of users to properly use their e-mail client software is critical. However, as this study's data has shown, most users do not have the knowledge required to make informed decisions about the attachments they receive.

There are a variety of aspects of e-mail management currently left to the user: including trust of the e-mail source, identification of the appropriate file type, and the decision regarding opening of that attachment. Without ensuring that users can perform these actions in a knowledgeable manner, the Coast Guard leaves itself susceptible to malicious code infection through e-mail.

Addressing the first concern, users cannot be relied upon to trust the source of a given e-mail. In order to ensure that identity of an e-mail sender, the use of Public Key Encryption systems that allow for both digital signatures and encryption exist. Unfortunately, current methods of securing e-mail do not necessarily provide great relief for users. Whitten and Tygar [Ref. 5] found that a significant number of users were unable to successfully use a common e-mail encryption tool despite the fact that subjects had access to the manual for the software used. Some software packages that allow for signing and encryption act as plug-in features within current e-mail client software. In the case of Microsoft Outlook, the Coast Guard's standard e-mail application, these features usually work as button-based icons similar to those used for file attachments. Based upon their own experiences, 53% of the study's participants felt that they would inadvertently forget to sign e-mail if the application was configured to require explicit

user action for signing. Likewise, 53% felt that merely setting encryption and signatures as the system's default setting would not be acceptable if it made their e-mail unreadable or unusable by some outside recipients.

Assuming that users do trust the source of the e-mail, the contents of any attachments are also subject to scrutiny due to the nature of many of today's viruses such as the ILUVYOU and Melissa viruses. Since, as mentioned in Chapter III, filtering all potentially harmful attachments may not be a viable solution, users are left with the responsibility of determining whether they should trust these on their own. The data presented in this survey demonstrates that at this time, most users are not prepared to do so. Failing to educate users regarding methods for making these determinations will result in continued virus infections and some users over-filtering attachments out of fear. Both of these results have an adverse impact on business practices and point to the need for better education in this area.

For remote connections and for data exchanged from users' homes, the Coast Guard must also rely upon its personnel to maintain up-to-date security patches, including virus definitions. Since the Coast Guard does not control users' systems outside of work, awareness once again becomes critical. If users are unaware of patches, virus definition updates, and installation procedures, they will be unlikely to use them. Some businesses and government organizations have even purchased extended licenses for virus software to cover users home systems. Even though these programs allow for the free use of the software by the individuals, the systems still rely upon those users actually installing and periodically updating the software, and they may be unwilling to do so if they fail to perceive a threat to their own or the Coast Guard's systems.

3. Interface Issues

As demonstrated in both the e-mail exercise and the SSL questions of the survey, the current Windows user interface does not provide most users with the information they need to make informed security decisions. Instead, cryptic security warnings tend to further confuse users with most failing to understand their meaning. Left with the choice of trusting a system they don't understand or not using that system, most users seem to err toward the latter choice. Refusing to use new systems is not an option that will allow the Coast Guard to capitalize on technology.

Ideally, new interfaces would be developed that incorporate easily understood security features within their design. This does not appear to be the case for the near future, and as new applications are developed, so to will new security concerns arise.

Instead of relying upon plug-in solutions, users should be made aware of the security implications of the applications they use. Whether e-mail, a web browser, or a Coast Guard database application, each has unique security features and concerns associated with it. Allowing users to blindly use these applications without introducing them to these features only heightens the risk they pose, whereas indoctrinating them into the proper use of all of the applications they use fosters proper use as the rule vs. the exception.

C. INCREASING USER AWARENESS

While there are a number of measures that can be taken to address specific security concerns and practices, each of those solutions requires proper participation by the user in order to be implemented effectively. Smart cards require users to take physical security precautions, virus definitions must be updated, and trust relationships

must be formed. Regardless of the technology used, as long as there is a human element involved in the transaction, user awareness will play a key role in ensuring those systems remain secure. This only reinforces the emphasis that companies have placed on user awareness as a hindrance to their ability to implement security solutions [Ref. 11 & 12].

There are numerous ways to attempt to increase the security awareness level within an organization. In the military, many of the attempts to raise security awareness stem from military intelligence concerns as demonstrated by the Security Awareness Training and Education (SATE) program. The SATE program was established to help people "recognize, understand and accept the need to protect government assets," and it specifically identifies this need with respect to classified information, property, and personnel. In addition, Coast Guard members are exposed to a variety of other awareness programs such those for medical mishaps, crime prevention, and boating safety. Key to each of these programs is that they are designed to bring about a vigilant attitude in users so that knowledge of the program's subject matter is always consciously available.

Identifying the methods best suited for the Coast Guard in increasing user awareness entails a combination of many factors including the program cost, the willingness of users to participate, and the actual effectiveness of the program with regard to increasing awareness. Table 1 provides details regarding user perceptions, perceived effectiveness, and the estimated cost (in time and funding) of implementing 10 program options presented to the survey participants.

Program Name	Willingness to Participate	Program Effectiveness	Relative Cost of Implementation
Formal Training	1	1	High
Online Testing	3	7	Low to Moderate
Lessons Learned	5	6	Low
5-10% Coworker Training	2	2	Moderate
ESO Training Videos	8	9	Low to Moderate
FAQ Website	4	5	Low
Awareness Posters	10	10	Low
Instant Message Help	6	3	Low to Moderate
Sys Admin Password Cracking	9	8	Low to Moderate
Live Hack Demos	7	4	Moderate

Table 1. Assessment of Methods to Increase Awareness

Rankings were calculated using weighted averages, based upon participant responses for each of the identified programs while relative cost information is an estimation of the cost of implementing any awareness program on a Coast Guard-wide basis. The ranking scale ranges between 1, the most effective program, to 10, the least effective.

From the table, participants perceived the most desired and effective program to be one using required formal training. However, any such program would also be extremely expensive to implement for all users in the traditional sense of classroom-based training.

Alternatively, advanced training for 5-10% of workers could prove to be extremely beneficial to the Coast Guard. Participants perceived this option as second highest in both effectiveness and in their willingness to see it implemented. In addition, since a significant proportion of the participants stated that they seek coworker guidance for their questions and problems, this advanced training could assist ensuring that users receive proper guidance in these situations.

One potential disadvantage of this method would be an increase in the "technology divide" perceived by a number of users. Several users made comments on their surveys and verbally regarding double standards among users since IT personnel were able to install software, access features, and perform services from which "normal" users were restricted. As one user stated, "All aren't treated fairly. We're told not to do something regarding the computer, but others 'in computers' are allowed to." This perception also led to lower levels of trust by users since some members didn't trust their administrators since, "all files can be viewed locally by TC's. (You can't store anything that) you don't want others to see."

Properly implemented, training office coworkers could assist in easing instead of aggravating these feelings. Since members of their own work group could be granted increased system access privileges based upon their level of knowledge and training, the perceived divide between IT workers and the average workers would be seen as less extreme.

The third most desired program was that of periodic online testing. Depending upon its implementation, this can provide a quick, objective means of assessing user knowledge regarding key security concepts. The Naval Postgraduate School has used such a program to ensure that users understand various system use policies. Constructed with links to reference material, and capitalizing on online education techniques, systems such as this can validate knowledge the user has and reinforce understanding of apparent weaknesses.

Many users currently feel the effectiveness of such programs offers little promise, and with regard to effectiveness, they ranked this program as the 7th of the 10 possible

solutions they were given. However, the fact that it was ranked as third with regard to user willingness to participate seems to bode well for the Coast Guard's recently introduced program which allows users access to online education courses. If significant numbers of personnel take advantage of these opportunities and have favorable experiences in doing so, perceptions regarding program effectiveness could improve.

Participants felt that the third and fourth most effective programs would be the use of a security "Answer Man" and the use of hacking technique demonstrations. However, even though they felt these measures would prove to be effective, their willingness to participate in such programs was below average. Some of this appears to be due to lack of familiarity with the systems, and in the case of the hacking demonstrations, a feeling that it could lead to more harm than good.

Corporations, such as American Airlines (http://www.aafltsvc.com/fsoperations) have used instant messaging with some success to answer questions from remotely located employees. Allowing users to receive just-in-time answers to their questions from a live person can assist in building user trust in the systems, and the interactive nature achieves this much more effectively than e-mail which can be subject to undue delays and often provides no indication that it has either been read or even received [Ref.16]. Assuming that staff members could maintain active participation in such a program, whether using instant messaging or online chat format, the potential to provide users with policy-based answers to questions and concerns appears promising. However, due to the lack of familiarity and trust of many users in such programs, initial experiences would prove critical to building user trust in the system. If the system fails to meet user expectations, the likelihood that they would use such a program would decrease.

Since hacking demonstrations also face user reluctance, care should be taken in implementing programs of this nature as well. One possible solution would be to combine this solution with that of the advanced training of 5-10% of personnel. From the author's personal experience, practical demonstrations have proven critical toward demonstrating just how easily systems can be compromised and how much the systems depend upon users awareness. Exposing selected members to these techniques would provide greater exposure of the user population to existing potential threats, and these users could in turn assist in increasing the awareness level of other users within their work environment.

Many of the lower cost solutions are perceived by users to be of little or no value. Among these were the use of awareness posters and Educational Service Officer (ESO) training videos. Discussions with personnel indicated that these measures would fail to draw their attention and go unused respectively. Based upon the user apathy toward these solutions, and unless there are clear indications to the contrary, it appears that any awareness funding would be better spent on other efforts.

Users themselves recognize that they're security awareness is important to their jobs, with 67% of personnel surveyed feeling that they could perform their duties more safely and effectively if they're awareness level was higher. Taking advantage of the techniques described above, positive steps toward increased user awareness should be possible.

Assuming that user awareness can be heightened, other perceptions can also influence the success of a security program. If users are fully aware of concerns, but feel that their business practices are not being supported, this can easily lead to user

frustration. The next section of this chapter will discuss user perceptions regarding the Coast Guard's security program and use of technology.

D. GENERAL USER PERCEPTIONS

When asked about the Coast Guard's security program, 64% of users felt that current security measures were neither too weak nor too strict, however, only 62% of users felt the Coast Guard was taking full advantage of current technology. When queried further, many of the comments provided by users indicated areas where security concerns seem to be hindering factor in the use of technology. The two chief areas of concern expressed by users were remote access restrictions and software installation barriers.

1. Remote Access Restrictions

There were a variety of users who felt their performance was hindered by their inability to remotely access files, e-mail, and other applications. Many personnel working in congested areas cited desires to telecommute, or at least access files and e-mail after hours. Others cited direct, operational needs to remotely access systems including the ability to send photographs and information from accident sites, accessing Coast Guard databases when conducting remote inspections, and the lost work product resulting from discontinuity in service when traveling.

Increasing numbers of users are discovering the potential for remote access to enhance their operational abilities. These enhancements are further complimented by the positive impact that they can have on workers' quality of life. If users perceive that only security policy prevents them from taking advantage of such technology, especially if they are not fully apprised of the concerns for doing so, this will only lead to heightened

frustration and a greater perceived divide if technology workers seem to be the only personnel who can access systems remotely.

2. Software Installation Barriers

Another common concern was the Coast Guard's policy preventing the installation of software unless the software configuration has been tested and approved for use on the Standard Workstation III. Unfortunately, gaining approval for any such software is a long and tedious process and for many applications, Coast Guard users do not perceive any security threat and become easily frustrated.

The clearest example of user frustration in this respect stems from the Coast Guard's own web cast of a public meeting in December 2000. Field units were encouraged to participate in this event but Real Player, the required software to view the web cast, was not an approved software package. After extensive complaints, the unit involved was granted permission to temporarily install the Real Player software as long as it was uninstalled upon completion of the web cast. Frustration levels at the unit were high enough to warrant the unit writing a letter to Coast Guard Headquarters regarding the situation.

Since the Coast Guard's migration to a Windows platform, user familiarity with that environment has led to a thirst to take advantage of the increased capabilities these systems have. A successful security program cannot allow itself to be perceived as a hindrance to technological advancement. In the minds of users, doing so constitutes a self-imposed denial of service and it damages users' trust and willingness to participate in effective security measures.

E. CONCLUSION

Information Security awareness is a problem in the Coast Guard just as it is in the commercial sector. No security program can succeed without the willing and knowledgeable participation of the personnel involved. In the Coast Guard, this is all the more critical since its multi-mission environment combines the security concerns of military intelligence, law enforcement, and regulatory body under one consolidated organization.

Comparing Coast Guard user perceptions and practices with known potential problem areas, allows for an assessment of user awareness with regard to these areas of concern. In doing so, this study found that Coast Guard personnel appear susceptible to a number of threats which target the human element in information security including: weaknesses in password practices; limited compliance with policy; poor knowledge of virus characteristics and behavior; and misapplications of trust. In addition, the study found that user perceived information security measures as preventing the implementation of some key technologies that would benefit them both personally and operationally.

In order to balance the ability of the Coast Guard to take advantage of emerging technology while simultaneously ensuring the continued security of system resources, user awareness must be increased. While there are a number of potential solutions that could assist in developing that awareness, there are strengths, weaknesses, and costs associated with each option. Several proposed solutions, including advanced training for some users, online testing, and Internet messaging applications appear to provide good

value in terms of their cost, willingness of users to participate in the programs, and the perceived effectiveness of those programs.

Developing programs in which users willingly participate will be critical to the long-term effectiveness of any attempts to increase awareness. Current development efforts, such as the *Sim Security* information assurance awareness and training game being developed at the Naval Postgraduate School, offer promise in this area. Of equal import will be the elimination of the perception that security serves as a hindrance to conducting routine business practices effectively. Accomplishing both of these goals will greatly assist in enhancing user trust and will make the maintenance the Coast Guard's information security efforts a cooperative effort rather than a confrontation between IT personnel and "regular" users.

APPENDIX. HUMAN FACTORS SURVEY

The following pages form the survey administered to participants at each of the four selected Coast Guard units. Participants received full-color copies of the survey in an attempt to most accurately simulate screen characteristics, as they would present themselves.

Form ID Number:_____

Name:_____

E-Mail:_____

Information System Security Awareness Assessment

The purpose of this survey is to help the Coast Guard assess the organizations current awareness of computer and information system security. This assessment, while sponsored by TISCOM is being conducted independently with the hope of:

- Allowing users to obtain the most benefit from USCG Systems;
- Ensuring that security measures on USCG systems are actually useable by the average user and that they are appropriate to the system on which employed;
- Identifying the security awareness level within the USCG's user population;
- Assisting the USCG in focussing training and education efforts; and
- Assessing any perceived or real hindrances caused by the security measures currently in place.

We want to ensure that the answers, comments, and concerns that you provide are as honest as possible. For this reason, the results of this survey will be kept anonymous and answers will be consolidated in the form of statistical data. Your name is needed on this sheet for the purpose of obtaining possible follow-on information only (i.e. follow-on interviews or clarification of comments).

This is a survey-based assessment, not a test. No honestly provided answer is incorrect. When answering the questions, some questions may seem to have a similar focus. Some may cause a desire to change previous answers. Each question should be answered individually and, once answered, please try to avoid any tendency to go back to "re-answer" a question.

Comments are encouraged. While the majority of the questions are of a multiple-choice format to aid in statistical counts, this can limit the ability to identify all situations. Comments which identify the question can aid in improving the survey and in addressing your concerns (Example: Question 3: "Specialty" – I am a Marine Inspector but have the collateral duty of System Administrator.). Please select the best possible answer and provide your comments in the space provided at the end of the survey.

I have read the above information, understand the purpose of this survey, and am willing to participate. I understand that I may be contacted by the interviewer in the future for clarification or additional information.

- ☐ I am interested in participating in further aspects of this study.

_____

Signature

Form ID:_____ Unit:_____

Grade:_____

Specialty:

◊ Vessel Ops o Afloat o Ashore	◊ Marine Safety o Inspections o REC o Investigations o MEP	◊ Administrative (Including Supply, Personnel, Clerical, & similar positions)
◊ Aviation o Crewmembers o Support Personnel	◊ Other _____	◊ Info Tech Related

General Usage Questions

	1 No Experience	2 Little	3	4 Average Skill Level	5	6 Power User Level	7 Professional Level
1. I consider my general computer skills to be:	o	o	o	o	o	o	o
2. My knowledge of computer security issues is:	o	o	o	o	o	o	o
3. To perform my job adequately, I feel my skill level should be:	o	o	o	o	o	o	o
4. Most of the other people in my work group have skills of:	o	o	o	o	o	o	o

5. When I have a general computer (formatting, sending e-mail, etc...) use question, I typically:

- o Work to find the answer myself.
- o Seek the guidance of a coworker within my workgroup.
- o Seek assistance from system administrator.
- o Ignore it or seek a "workaround."

6. When I have a computer *problem*, (crashing, erratic system behavior, etc...) I typically:

- o Work to find the answer myself.
- o Seek the guidance of a coworker within my workgroup.
- o Seek assistance from system administrator.
- o Ignore it or seek a "workaround."

Question	Yes	No
7. I know where there are copies of user manuals for the computer software I typically use.	O	O
8. I know the policy regarding who is authorized to use USCG computer resources and for what purposes they may use them.	O	O
9. I know the USCG policies regarding passwords (selection, changing, compromise, etc..).	O	O
10. I know the USCG policies regarding e-mail use (appropriate use, attachments, reporting suspicious, etc…)	O	O
11. I feel that the policies in questions 8 - 10 are followed.	O	O
12. If I have questions regarding USCG policies in these areas, I know where to find copies.	O	O
13. I know who at my unit supervises these issues.	O	O
14. I feel comfortable approaching them with questions/issues in these areas.	O	O
15. I sometimes receive e-mail from people I don't know.	O If yes, approximately how many times per week ____	O
16. I sometimes receive unsolicited, commercial e-mail (a.k.a. spam) at work.	O If yes, approximately how many times per week ____	O
17. I typically open and read all e-mail I receive.	O	O
18. I typically open all attachments I receive.	O	O
19. I know what to do if I receive a *suspicious* e-mail.	O	O
20. I know what constitutes a *suspicious* e-mail.	O	O

Question	Yes	No
21. I receive and read jokes, cartoons, pictures, stories, and other similar material via e-mail from friends.	O	O
22. I don't worry about my e-mail attachments since the USCG uses virus protection software.	O	O
23. I sometimes use the Internet at work for personal use.	O	O
24. I use Internet messaging software (AOL Instant Messenger, Yahoo! Messenger, MSN Messenger, ICQ, etc…) at work.	O	O
25. I trust the way that the current ADC is posted online.	O	O
26. I always log off or lock my workstation when I leave my workspace.	O	O
27. I have a home computer or have access to one outside of work.	O	O
28. I exchange material via disk, e-mail, or other means between work & another location (i.e. bring work documents home or home/school material to work).	O	O

29. I use the following types of computer software:

(check all that apply including use at home, work, or other location)

- o MS Word (or other word processor)
- o MS Excel (or other spreadsheet)
- o MS Access (or other desktop database)
- o Internet Explorer or Netscape Navigator
- o E-mail (Outlook, Eudora, Outlook Express, etc…)
- o Windows 95/98/Me
- o Windows NT
- o Linux / UNIX
- o Macintosh OS
- o Telnet
- o FTP
- o Web Development (FrontPage, etc…)
- o USCG Applications (MSIS, LEIS, PERSRU software, Supply/Budgeting, etc…)
- o Other: Please list

30. At home, I check for operating system updates:

O Relatively Frequently (at least monthly) O Seldom (less than once per month)
O Only when I hear about a bug on the news O Never O Other (describe below)
O I don't need to since I always use the newest software like Windows Me

Passwords and System Access

31. At work, I have _____ different passwords (including account PIN's). (Please enter a number)

32. At home, I have_____ different passwords (including account PIN's). (Please enter a number to include web sites at which you may have registered)

Question	Yes	No
33. I work with at least one system that automatically generates random passwords:	O	O
34. I sometimes have difficulty remembering passwords for different accounts.	O	O
35. Currently or in the past, I've written passwords down.	O	O
36. My unit currently, or in the past, has required, encouraged, or "looked the other way" with regard to password sharing to assist in productivity.	O	O
37. Currently or in the past, I've shared one of my passwords.	O	O
38. I've been given a coworker's password before so that I could access files, applications, etc…	O	O
39. For USCG systems, I typically select passwords which are the same or very similar to each other.	O	O
40. When I register at a web site, I typically select passwords which are the same or very similar to those I use for USCG systems.	O	O
41. I have written down and carried a bank/credit card PIN in my wallet or on my person.	O	O
42. I have been locked out of a system or website because I forgot or used the wrong password.	O	O

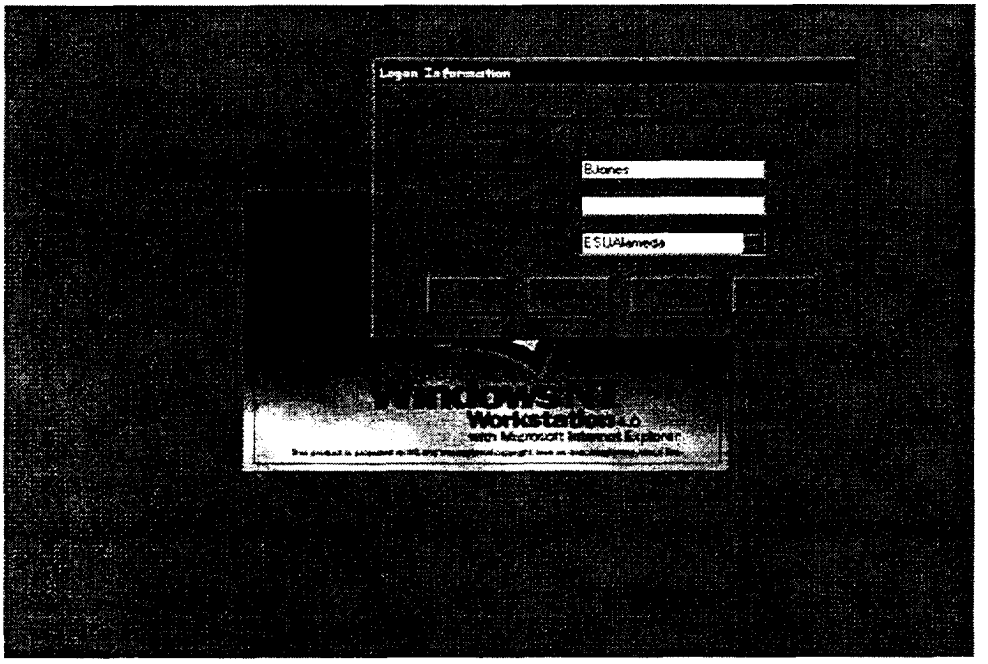
43. With regard to any passwords that you have created in the last year (**check all that apply**):
- O They contain sequences of 4 or more letters
- O Contain English or foreign words
- O Contain words spelled backwards
- O Contain names (people or locations) or initials
- O Contain acronyms (USCG, SAR, NRA, etc…)
- O Are a variation of your user name
- O Contain anything publicly available about you or your family such as license plate number, address, phone number, SSN, birth dates, anniversaries, etc…)
- O Contain "keyboard strings" (i.e. qwerty, asdf, 4567, etc…)
- O Uses a common bible citation (e.g. John3:16) or other literary reference (e.g. 4score&7)
- O Created by interrelating previous passwords or passwords from other systems (i.e. Xmen10 for one password and Xmen11 and Xmen12 as others)

44. If I suspect that my password has been compromised on Windows NT or if I want to change it for any other reason, I would:
    O Have to wait until end of password valid period until password expires & change required at logon.
    O Have to inform the system administrator since only they can change a password before expiration.
    O Go on as normal since I wouldn't want to admit password loss or don't feel any harm done.
    O Change password myself if so, please briefly describe below how you believe this is done.
    O Other please describe below.

_____

_____

45. You approach your machine and are presented with the following screen:

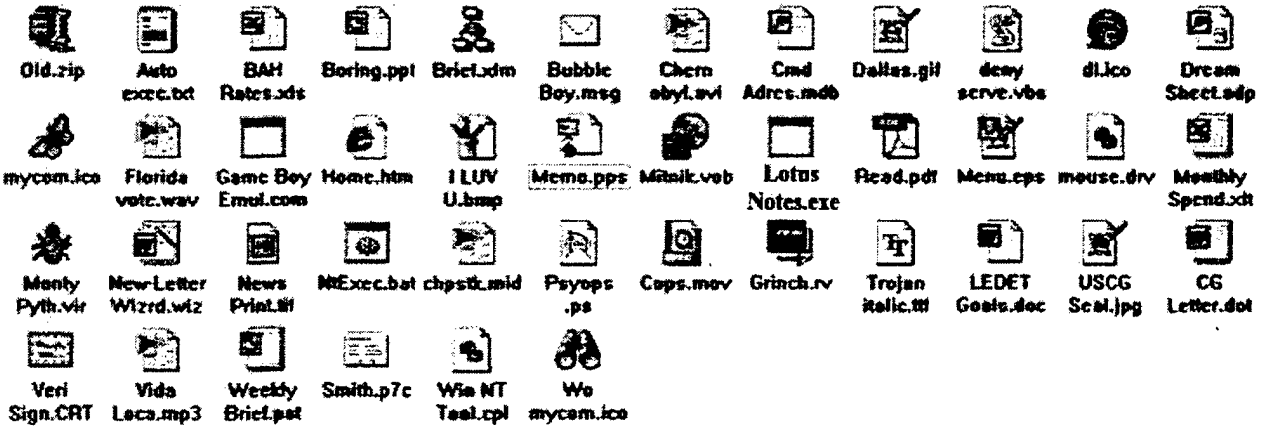


At this point, you should:
O Enter your user name and password. Click the "OK" button or press return to sign on.
O A hard reboot is always recommended at this point to clear the computer's memory since you were not the last user of the system.
O Press Ctrl-Alt-Del.
O Enter your user name and password. Change the computer's domain to the correct one for your unit by selecting from the drop down list. Click button or press return to sign on.
O Other. Please describe below.

_____

Viruses, Trojans, Spoofs, and other Malicious Code and Similar Threats

46. Circle the files below which you might suspect as being <u>potential</u> virus/malicious code carriers (i.e. the file is of a type known to be capable of containing malicious code).



47. T F Typical users don't need to worry about computer viruses since the USCG firewall & virus software are up to date & prevent them from affecting the systems.

48. T F If a system becomes infected with a virus, it is always obvious because either the system will stop working, bizarre effects will occur onscreen, or the a warning will be displayed by the Coast Guard's actively scanning virus software.

49. T F A weakness of malicious software including all keyboard loggers, password sniffing programs, and other similar programs is that they must be active in the system's memory and can be identified and shut down from the Windows NT task manager.

50. T F Users that limit their computer use to Microsoft Word, Excel, and Outlook are unlikely to become infected with a virus since viruses are most frequently contained in executable program files or are downloaded from the Internet.

51. T F Viruses spread so rapidly that it is critical to get the word out quickly. To help prevent this, Coast Guard policy states that if you are the first to receive a virus warning via e-mail, you should forward it to all members of your command as well as to FlagPlot@comdt.uscg.mil so that preventive measures can be taken.

52. T F If I receive an e-mail at work, I know that it and any attachments really came from the sender since the firewall filters out all "spoofed" e-mail.

53. T F If I suspect that my system has a virus, the best practice is always to shut down the system, remove any floppy disks, and reboot the system to limit the virus' spread.

54. Do you have virus protection software installed on your home computer and other non-work computer systems? (Circle One) **Yes** **No**

If yes, how often do you update the virus definitions?
O Weekly or less O At least once each month O Occasionally
O When I hear about a new virus O Never O Set to Automatically update

If your software is set to automatically update, do you (check all that apply):
O Leave the system on at all times O Use a dial-up Internet connection
O Have your ISP password stored on your system
O Occasionally manually check the system's virus definition date

55. Do multiple people (family members, etc…) have access to your home/other systems? **Yes** **No**

56. Do multiple people install software, access the internet, or download files on your home/other system?
O No, only I perform these activities. O Sometimes, but only with my knowledge.
O I'm not certain what other users do. O Yes, this is normal.

57. In general, the other users of the non-work systems I use are:
O Less familiar with computers O Equally Familiar O More Familiar

58. With regard to hardware connections to my computer systems (**Check all that apply**):

O I am familiar with, and frequently check these connections on my **work** computer.
O I am familiar with and frequently check these connections on my non-work computers.
O I am familiar with but don't check these connections often.
O The wiring to at least some of my systems is a mess or is hidden and difficult to assess.
O At work, new hardware connections would have to be installed by a system administrator and so are of little or no threat.
O I have seen or heard of hardware-based keystroke logging items such as Key Ghost.

Internet Security, Digital Signatures, and Encryption

Figure A and Figure B below are 2 examples of the many Internet web sites which request that you submit personal and/or financial information over the Internet.

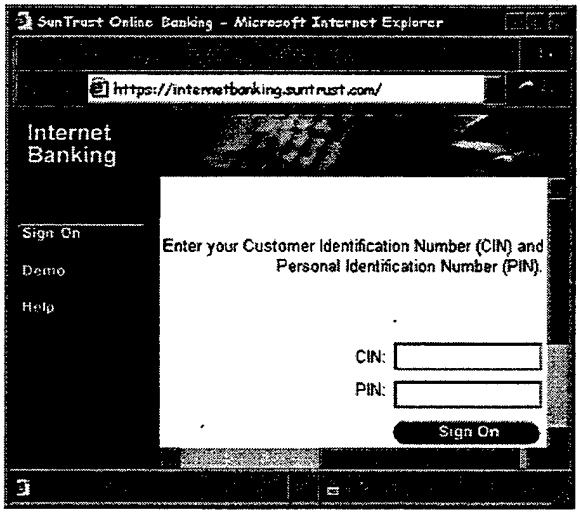


Figure A

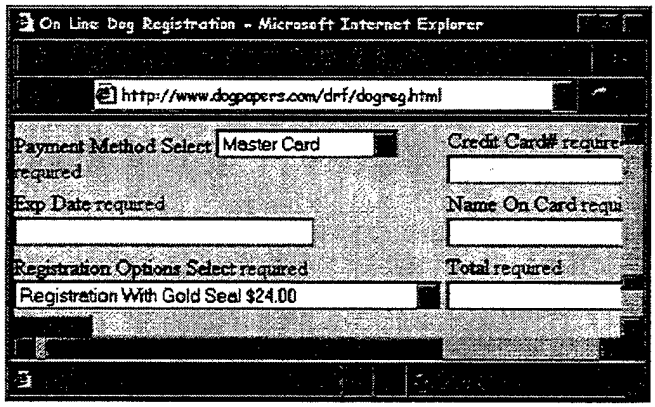


Figure B

59. Do you feel that it would be **safe** to submit information over the Internet using the site displayed in Figure A? (Circle One) **Yes** **No**

60. Would you *feel comfortable* submitting information using the site displayed in Figure A? **Yes** **No**

61. Do you feel that it would be **safe** to submit information over the Internet using the site displayed in Figure B? (Circle One) **Yes** **No**

62. Would you *feel comfortable* submitting information using the site displayed in Figure B? **Yes** **No**

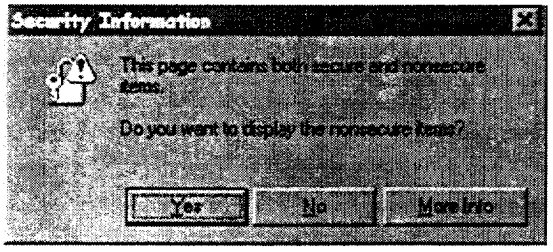
63. Please explain why you answered the previous 4 questions the way you did:

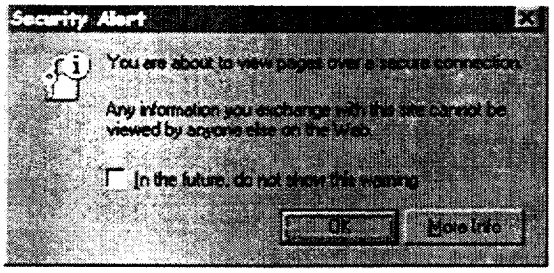
---

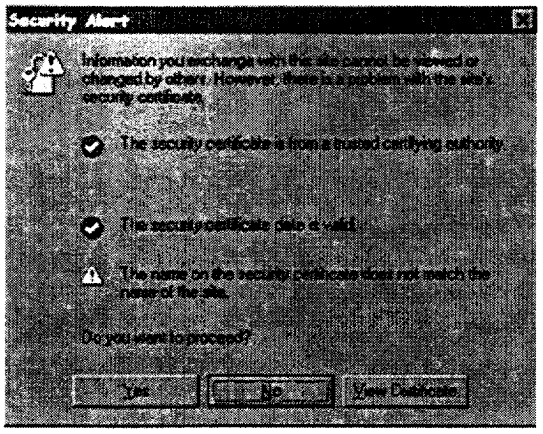
64. In the lower right hand corner of Figure A is a small padlock  . What does this let you know about the web site?

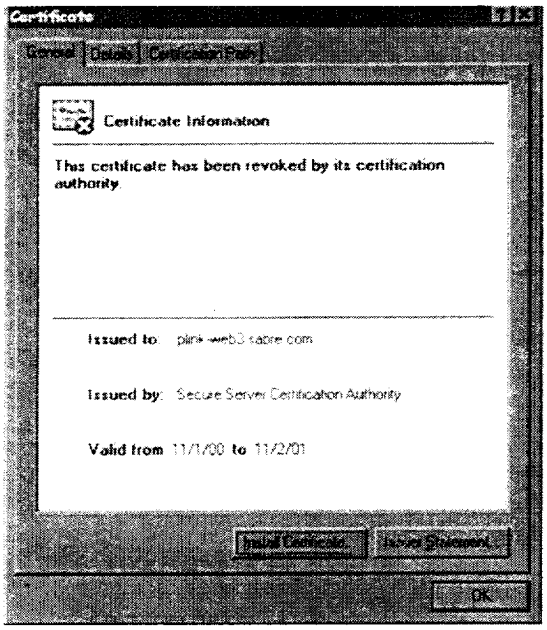
65. With regard to Figure A, if you wanted to obtain more information about the method of providing security for this site, how would you go about doing that?

66. When using the Internet, many times you may be presented with various message and dialog boxes concerning the security of the sites you visit. Below are some of the items which you might see. To the right of each, please describe how you would handle each, whether you would be concerned, if you would ignore them, etc... (Not being sure what to do is a completely appropriate answer).









Question	Yes	No
67. Do you ever receive e-mail in which the sender inadvertently forgets to include the attachment?	O	O
68. Have you ever inadvertently forgotten to include an e-mail attachment?	O	O
69. Considering the last 2 questions, if you were occasionally required to digitally sign or encrypt e-mail, & doing so required you to remember to click an additional button before sending, do you think you might inadvertently forget to do so before sending?	O	O
70. Not all e-mail systems recognize all digital signatures & encryption formats making your e-mail unreadable by some recipients. Knowing this, do you feel that a default setting that signs and encrypts all e-mail would be a viable solution?	O	O
71. Often, digital signature/encryption keys are stored on a user's computer. If you installed a key on your personal computer, do you feel comfortable that you would understand how to secure it to prevent accidental or intentional use by others?	O	O
72. Would you feel comfortable/safe using smart cards for signing/encryption?	O	O
73. Would you feel comfortable using optical scanners or other biometrics?	O	O

Measures to Improve Security Awareness

74. As you may have determined from this survey, there are many factors to consider with regard to Computer Security issues, and user awareness plays a key role in many of these areas. There are a number of ways to attempt to increase the general awareness level of the USCG's user base. Below is a list of potential formats to use in increasing awareness levels. Each item is followed by two spaces. In the first space, please rank order the list of education alternatives in the order, 1 through 10, that you personally would prefer to experience them (i.e. If you would most prefer mandatory formal training, mark this as **1**. If your second choice would be to receive e-mail notices regarding security issues, mark this **2**, etc... until the list is exhausted). In the second space, please rank what you feel the likely effectiveness of this type of education from 1 (completely ineffective) to 7 (extremely effective). A ranking of "4" should be considered to be of average effectiveness.

Category	Rank	Effectiveness	Category	Rank	Effectiveness
Required Periodic Formal Training on Computer Security.	_____	_____	Maintaining a Frequently Asked Questions web site for security issues.	_____	_____
Requiring personnel to periodically review and take a short online test covering USCG computer security policy.	_____	_____	Publishing posters of which highlight computer security issues (possibly humorous/McGruff "take a bite out of crime" style).	_____	_____
Publishing periodic, humorous summations of security "lessons learned" similar to current medical mishaps messages.	_____	_____	Having a computer "answer man" available via live chat, AOL instant messenger, or other means to answer user concerns in real time.	_____	_____
Providing advanced training to approximately 5 - 10% of average office users so they could better answer/assist coworkers.	_____	_____	System administrators using password cracking programs to identify users with weak passwords	_____	_____
Providing ESO's with copies of educational computer security videos.	_____	_____	Live demonstrations of hacking techniques and how to prevent them.	_____	_____

Question	Yes	No
75. In general, are you comfortable with your knowledge of computer security?	O	O
76. Do you feel USCG security policy is too strict or extensive?	O	O
77. Do you feel USCG security policy is too weak?	O	O
78. Do you feel that you could perform more safely/effectively if you better understood computer security issues?	O	O
79. Do you feel that the USCG is taking the best advantage of current technology?	O	O

80. What measures would you like to see implemented to improve security awareness?

_____

_____

_____

_____

81. Do you know of any current technology that it appears the USCG is not fully taking advantage of, possibly due to security concerns? (Examples: Are remote/home network access policies too restrictive? Is there software that could improve job performance that you are not allowed to install on your work system?)

_____

_____

_____

_____

82. Do you trust the security of the USCG's computer systems? Why or Why not?

_____

_____

_____

_____

Comments

Please use the following space to provide any additional comments you would like to express or to more fully explain an answer to a previous question to which you would like to provide comments. You may continue on the back if you need additional space.

_____

_____

_____

_____

_____

_____

_____

_____

THANK YOU FOR PARTICIPATING IN THIS SURVEY

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Department of the Navy, Fleet Information Warfare Center, *Navcirt Advisory 00-24 – Computer Security Hot Topics*, July 2000.

2. United States Senate, *Report 106-259, Government Information Security Act of 1999,* April 10, 2000.

3. United States General Accounting Office, *Computer Security, Critical Federal Operations and Assets Remain at Risk,* September, 11, 2000.

4. United States General Accounting Office, *Information Technology Management, Coast Guard Practices Can Be Improved,* December 12, 2000.

5. Whitten, Alma and Tygar, J. D., *Usability of Security: A Case Study*, December 18, 1998.

6. Adams, Anne and Sasse, Martina Angela, "Users Are Not the Enemy," *Communications of the ACM,* Vol. 42, No. 12, December 1999.

7. Karvonen, Kristiina, "Creating Trust," *Proceedings of the 2nd Nordic Workshop on Security (NordSec '99),* Krista, Sweden, November 1999.

8. SANS Institute, *Mistakes People Make that Lead to Security Breaches,* http://www.sans.org/mistakes.htm.

9. DITnet Staff, "'Bad passwords' biggest threat to system security says Cisco," http://www.dit.net/ITNews/newsjune2000/newsjune76.html, June 22, 2000.

10. Vibert, Robert, "Infectable Objects," http://www.securityfocus.com/ September 2000.

11. Ernst and Young, *2nd Annual Global Information Security Survey,* 1998

12. The National Computing Centre, *The Business Information Security Survey, (BISS 2000)*, February, 2000.

13. United States Coast Guard, *Automated Information Systems (AIS) Security Manual*, COMMANDANT INSTRUCTION M5500.13A.

14. Interface Security, http://www.keyghost.com.

15. Microsoft Assistance Center, "Outlook E-Mail Security Update," http://office.microsoft.com/Assistance/2000/Out2ksecFAQ.aspx.

16. Olson, Judith S., and Olson, Gary M., "i2i Trust in E-Commerce," *Communications of the ACM,* Vol. 43, No. 12, December 2000.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Suite 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Carl Siel 1
   Space and Naval Warfare Systems Command
   PMW 161
   Building OT-1, Room 1024
   4301 Pacific Highway
   San Diego, CA 92110-3127

4. Commander, Naval Security Group Command 1
   Naval Security Group Headquarters
   9800 Savage Road
   Suite 6585
   Fort Meade, MD 20755-6585
   San Diego, CA 92110-3127

5. Ms. Deborah M. Cooper 1
   Deborah M. Cooper Company
   P.O. Box 17753
   Arlington, VA 22216

6. Ms. Louise Davidson 1
   N643
   Presidential Tower 1
   2511 South Jefferson Davis Highway
   Arlington, VA 22202

7. Mr. William Dawson 1
   Community CIO Office
   Washington DC 20505

8. Capt. James Newman 1
N64
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202

9. Mr. Richard Hale 1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

10. Ms. Barbara Flemming 1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

11. CDR William M. Randall, USCG 1
Chief, Telecommunications Operations Division
Telecommunications & Information Systems Command
7323 Telegraph Road
Alexandria, VA 22315-3940

12. LCDR Jan Stevens, USCG 1
Chief, System Military Force Management Division (G-SRF)
United States Coast Guard Headquarters
2100 Second Street SW
Washington, D.C. 20593

13. United States Coast Guard Headquarters Library 1
2100 Second Street SW
Washington, D.C. 20593

14. Timothy J. Whalen, LT, USCG 1
915 West 90th Terrace
Kansas City, MO 64114